

1 Steve W. Berman (*pro hac vice*)  
2 Robert F. Lopez (*pro hac vice*)  
HAGENS BERMAN SOBOL SHAPIRO LLP  
1918 Eighth Avenue, Suite 3300  
3 Seattle, WA 98101  
Telephone: (206) 623-7292  
4 Facsimile: (206) 623-0594  
steve@hbsslaw.com  
robl@hbsslaw.com

5  
6 Bruce L. Simon (96241)  
Daniel L. Warshaw (185365)  
William J. Newsom (267643)  
7 PEARSON SIMON & WARSHAW, LLP  
44 Montgomery Street, Suite 2450  
8 San Francisco, CA 94104  
Telephone: (415) 433-9000  
9 Facsimile: (415) 433-9008  
bsimon@pswlaw.com  
dwarshaw@pswlaw.com  
wnewsom@pswlaw.com

10  
11 *Counsel for Select Plaintiffs and*  
*Co-Lead Counsel for the Proposed Classes*

12 [Additional Counsel Listed on  
13 Signature Page]

14 UNITED STATES DISTRICT COURT  
15 NORTHERN DISTRICT OF CALIFORNIA  
16 SAN FRANCISCO DIVISION

17 ) No. 12-md-2330-EMC  
18 IN RE )  
19 CARRIER IQ, INC., ) SECOND CONSOLIDATED  
CONSUMER PRIVACY LITIGATION. ) AMENDED COMPLAINT  
20 )  
21 )  
22 )  
23 )  
24 )  
25 )  
26 )  
27 )  
28 )  
-----)

**TABLE OF CONTENTS**

	<u>Page</u>
I. INTRODUCTION.....	1
II. JURISDICTION .....	2
III. PARTIES .....	3
IV. FACTUAL BACKGROUND .....	11
A. Revelations and Deep Concerns Regarding Carrier IQ Software .....	11
B. Carrier IQ Software as Deployed .....	16
1. The enormous number of affected devices.....	16
2. Carrier IQ Software's interception and transmittal of private communications and content .....	18
3. The FTC's investigation of, and actions against, HTC involving Carrier IQ Software.....	24
4. Further Comments on Carrier IQ Software .....	29
V. CLASS ALLEGATIONS .....	30
VI. CLAIMS FOR RELIEF.....	32
VII. PRAYER FOR RELIEF.....	129
VIII. JURY TRIAL DEMANDED .....	131

1 For their complaint against the defendants, plaintiffs allege as follows:

2 **I. INTRODUCTION**

3 1. This proposed class-action lawsuit concerns Carrier IQ Software, which is, or has  
 4 been, installed on millions of Americans' mobile devices. "Carrier IQ Software" is an overarching  
 5 term for Carrier IQ's "IQ Agent" and another software component, called the "CIQ Interface," that  
 6 is installed with the IQ Agent in the software's most popular deployment. Though the defendants in  
 7 this suit describe the Carrier IQ Software as a benign tool installed at the behest of wireless carriers  
 8 to help them provide better service, the defendants have intentionally designed and deployed it to  
 9 do far more than gather data regarding signal strength or dropped calls. Far from designing the  
 10 software to collect bland metrics alone, they have designed and deployed it such that it also  
 11 intercepts private communications, content, and data, including: URLs<sup>1</sup> containing HTTP and  
 12 HTTPS query strings<sup>2</sup> embedded with Internet search terms (that might, for example, reveal  
 13 consumers' medical conditions, sexual orientation, religion, or a host of other personal  
 14 information), user names, passwords, and granular geo-location information; granular geo-location  
 15 information apart from that transmitted in URLs; SMS text message content; and application  
 16 purchases and uses. In fact, due to the design choices intentionally effected by the defendants, the

---

18 <sup>1</sup> "In computing, a uniform resource locator (URL) is a specific character string that constitutes a  
 19 reference to a [web] resource." See [http://en.wikipedia.org/wiki/Uniform\\_resource\\_locator](http://en.wikipedia.org/wiki/Uniform_resource_locator) (last  
 accessed June 23, 2014).

20 <sup>2</sup> "In the World Wide Web, a query string is the part of a uniform resource locator (URL) that  
 21 contains data to be passed to web applications such as CGI programs. When a web page is  
 22 requested via the Hypertext Transfer Protocol [HTTP], the server locates a file in its file system  
 based on the requested URL." See [http://en.wikipedia.org/wiki/Query\\_string](http://en.wikipedia.org/wiki/Query_string) (last accessed June  
 23, 2014).

23 "The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative,  
 24 hypermedia information systems. HTTP is the foundation of data communication for the World  
 25 Wide Web." See [http://en.wikipedia.org/wiki/Hypertext\\_Transfer\\_Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (last accessed June 23,  
 26 2014).

27 "Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure  
 28 communication over a computer network, with especially wide deployment on the Internet.  
 Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the  
 Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security  
 capabilities of SSL/TLS to standard HTTP communications." See  
<http://en.wikipedia.org/wiki/Https> (last accessed June 23, 2014).

Carrier IQ Software intercepts confidential and private content that the wireless carriers say they never wanted or requested, such that interceptions of such data was not done on their behalf.

2. Also, as explained more fully below, communications, content, and data intercepted by the Carrier IQ Software have been transmitted off mobile devices without the knowledge of consumers. In fact, in at least one deployment, some of this material, including SMS text message content, has been transmitted without consumers' knowledge to Google, the author of the Android mobile operating system; to one of the defendant device manufacturers; and probably to application vendors and developers as part of device or application crash reports. That deployment caught the attention of the Federal Trade Commission ("FTC"), which took action against the manufacturer involved.

3. Plaintiffs' rights to privacy and security in their confidential, private, and sensitive communications have been infringed, in violation of federal and state law. Furthermore, plaintiffs and members of the proposed class have suffered economic harm; they would not have purchased their mobile devices had they known that these devices bore hidden battery-, processor-, and memory-taxing software that intercepts private and confidential communications and enables them to be sent to unintended recipients.

4. Plaintiffs, on behalf of themselves and similarly situated mobile device owners, bring this suit under the Federal Wiretap Act, state privacy statutes, state consumer protection acts, the Magnuson-Moss Warranty Act, and state warranty laws for the maximum relief available to them and the proposed class.

## **II. JURISDICTION**

5. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because plaintiffs allege violations of federal law, including the Federal Wiretap Act as amended by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, and the Magnuson-Moss Warranty Act, 15 U.S.C. §§ 2301, *et seq.* The Court has supplemental jurisdiction over plaintiffs' state law claims pursuant to 28 U.S.C. § 1337(a).

6. This Court has personal jurisdiction over the defendants in this action because defendants are licensed to do business in the state of California or otherwise conduct business in California.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(b) inasmuch as unlawful acts are alleged to have been committed in this federal judicial district and defendants reside or regularly conduct business here. Furthermore, the Judicial Panel on Multidistrict Litigation, by order dated April 16, 2012, transferred all related cases in this matter to this Court for coordinated or consolidated pre-trial proceedings.

### III. PARTIES

## The plaintiffs

8. Plaintiff Patrick Kenny resides in Cave Creek, Arizona. Plaintiff Kenny purchased a Samsung Galaxy S 4G mobile device in 2011. He formerly owned and used an HTC Touch mobile device (“HTC Touch” is the name of that device, to the best of his recollection). Upon information and belief, Mr. Kenny’s devices came with the Carrier IQ Software and related implementing or porting software pre-installed. In addition to using his devices to make phone calls, Mr. Kenny used them for web browsing and text messaging, including accessing, inputting, and transmitting personal, private, confidential, and sensitive information. Mr. Kenny would not have purchased his mobile devices had he known that the Carrier IQ Software and related implementing or porting software was installed and operating on his devices, and taxing his devices’ battery, processor, and memory, as alleged herein.

9. Plaintiff Daniel Pipkin resides in Port Hueneme, California. Plaintiff Pipkin purchased a Samsung Galaxy SII 4G LTE mobile device in 2011. Upon information and belief, Mr. Pipkin's mobile device came with the Carrier IQ Software and implementing or porting software pre-installed. In addition to using his device to make phone calls, Mr. Pipkin has used it for web browsing and text messaging, including accessing, inputting, and transmitting personal, private, confidential, and sensitive information. Mr. Pipkin would not have purchased his mobile device had he known that the Carrier IQ Software and related implementing or porting software was

1       installed and operating on his device, and taxing his device's battery, processor, and memory, as  
 2       alleged herein.

3           10. Plaintiff Jennifer Patrick resides in Sacramento, California. Plaintiff Patrick  
 4       purchased a Motorola Bravo mobile device in 2010. Upon information and belief, Ms. Patrick's  
 5       mobile device came with the Carrier IQ Software and implementing or porting software pre-  
 6       installed. In addition to using her device to make phone calls, Ms. Patrick has used it for web  
 7       browsing and text messaging, including accessing, inputting, and transmitting personal, private,  
 8       confidential, and sensitive information. Ms. Patrick would not have purchased her mobile device  
 9       had she known that the Carrier IQ Software and related implementing or porting software was  
 10      installed and operating on her device, and taxing her device's battery, processor, and memory, as  
 11      alleged herein.

12           11. Plaintiff Dao Phong resides in San Francisco, California. Plaintiff Phong purchased  
 13      an HTC EVO mobile device in 2010. Upon information and belief, Ms. Phong's mobile device  
 14      came with the Carrier IQ Software and implementing or porting software pre-installed. In addition  
 15      to using her device to make phone calls, Ms. Phong has used it for web browsing and text  
 16      messaging, including accessing, inputting, and transmitting personal, private, confidential, and  
 17      sensitive information. Ms. Phong would not have purchased her mobile device had she known that  
 18      the Carrier IQ Software and related implementing or porting software was installed and operating  
 19      on her device, and taxing her device's battery, processor, and memory, as alleged herein.

20           12. Plaintiff Ryan McKeen resides in East Granby, Connecticut. Plaintiff McKeen  
 21      purchased a Samsung Epic Touch 4G mobile device in 2011. Upon information and belief, Mr.  
 22      McKeen's mobile device came with the Carrier IQ Software and implementing or porting software  
 23      pre-installed. In addition to using his device to make phone calls, Mr. McKeen has used it for web  
 24      browsing and text messaging, including accessing, inputting, and transmitting personal, private,  
 25      confidential, and sensitive information. Mr. McKeen would not have purchased his mobile device  
 26      had he known that the Carrier IQ Software and related implementing or porting software was  
 27      installed and operating on his device, and taxing his device's battery, processor, and memory, as  
 28      alleged herein.

1           13. Plaintiff Leron Levy resides in Miami, Florida. Plaintiff Levy purchased a Samsung  
 2 Moment mobile device in 2010. Upon information and belief, Mr. Levy's mobile device came with  
 3 the Carrier IQ Software and implementing or porting software pre-installed. In addition to using his  
 4 device to make phone calls, Mr. Levy has used it for web browsing and text messaging, including  
 5 accessing, inputting, and transmitting personal, private, confidential, and sensitive information. Mr.  
 6 Levy would not have purchased his mobile device had he known that the Carrier IQ Software and  
 7 related implementing or porting software was installed and operating on his device, and taxing his  
 8 device's battery, processor, and memory, as alleged herein.

9           14. Plaintiff Matthew Hiles resides in Davenport, Iowa. Plaintiff Hiles purchased an LG  
 10 Marquee mobile device in 2011. Upon information and belief, Mr. Hiles' mobile device came with  
 11 the Carrier IQ Software and implementing or porting software pre-installed. In addition to using his  
 12 device to make phone calls, Mr. Hiles used it for web browsing and text messaging, including  
 13 accessing, inputting, and transmitting personal, private, confidential, and sensitive information. Mr.  
 14 Hiles would not have purchased his mobile device had he known that the Carrier IQ Software and  
 15 related implementing or porting software was installed and operating on his device, and taxing his  
 16 device's battery, processor, and memory, as alleged herein.

17           15. Plaintiff Luke Szulczewski resides in Lansing, Illinois. Plaintiff Szulczewski  
 18 purchased an HTC EVO 4G mobile device in 2010. Upon information and belief, Mr.  
 19 Szulczewski's mobile device came with the Carrier IQ Software and implementing or porting  
 20 software pre-installed. In addition to using his device to make phone calls, Mr. Szulczewski has  
 21 used it for web browsing and text messaging, including accessing, inputting, and transmitting  
 22 personal, private, confidential, and sensitive information. Mr. Szulczewski would not have  
 23 purchased his mobile device had he known that the Carrier IQ Software and related implementing  
 24 or porting software was installed and operating on his device, and taxing his device's battery,  
 25 processor, and memory, as alleged herein.

26           16. Plaintiff Michael Allan resides in Liberty, Kentucky. Plaintiff Allan purchased an  
 27 HTC EVO 4G mobile device in 2011. Upon information and belief, Mr. Allan's mobile device  
 28 came with the Carrier IQ Software and implementing or porting software pre-installed. In addition

1 to using his device to make phone calls, Mr. Allan has used it for web browsing and text  
 2 messaging, including accessing, inputting, and transmitting personal, private, confidential, and  
 3 sensitive information. Mr. Allan would not have purchased his mobile device had he known that  
 4 the Carrier IQ Software and related implementing or porting software was installed and operating  
 5 on his device, and taxing his device's battery, processor, and memory, as alleged herein.

6       17. Plaintiff Gary Cribbs resides in Laurel, Maryland. Plaintiff Cribbs purchased a  
 7 Samsung Galaxy S2 Skyrocket mobile device in 2010. Upon information and belief, Mr. Cribbs'  
 8 mobile device came with the Carrier IQ Software and implementing or porting software pre-  
 9 installed. In addition to using his device to make phone calls, Mr. Cribbs has used it for web  
 10 browsing and text messaging, including accessing, inputting, and transmitting personal, private,  
 11 confidential, and sensitive information. Mr. Cribbs would not have purchased his mobile device  
 12 had he known that the Carrier IQ Software and related implementing or porting software was  
 13 installed and operating on his device, and taxing his device's battery, processor, and memory, as  
 14 alleged herein.

15       18. Plaintiff Shawn Grisham resides in Iuka, Mississippi. Plaintiff Grisham purchased a  
 16 Samsung Epic 4G mobile device in 2011. Upon information and belief, Mr. Grisham's mobile  
 17 device came with the Carrier IQ Software and implementing or porting software pre-installed. In  
 18 addition to using his device to make phone calls, Mr. Grisham has used it for web browsing and  
 19 text messaging, including accessing, inputting, and transmitting personal, private, confidential, and  
 20 sensitive information. Mr. Grisham would not have purchased his mobile device had he known that  
 21 the Carrier IQ Software and related implementing or porting software was installed and operating  
 22 on his device, and taxing his device's battery, processor, and memory, as alleged herein

23       19. Plaintiff Bobby Cline resides in Seabrook, New Hampshire, but at pertinent times to  
 24 this matter, he resided in Oakland County, Michigan. Plaintiff Cline purchased an LG LS670  
 25 Optimus S mobile device in 2011. Upon information and belief, Mr. Cline's mobile device came  
 26 with the Carrier IQ Software and implementing or porting software pre-installed. In addition to  
 27 using his device to make phone calls, Mr. Cline has used it for web browsing and text messaging,  
 28 including accessing, inputting, and transmitting personal, private, confidential, and sensitive

1 information. Mr. Cline would not have purchased his mobile device had he known that the Carrier  
 2 IQ Software and related implementing or porting software was installed and operating on his  
 3 device, and taxing his device's battery, processor, and memory, as alleged herein.

4 20. Plaintiff Mark Laning resides in Carrollton, Texas. Plaintiff Laning purchased a  
 5 Pantech P5000 mobile device in 2011. Upon information and belief, Mr. Laning's phone came  
 6 with the Carrier IQ Software and implementing or porting software pre-installed, and he was  
 7 notified that it was installed by Pantech. In addition to using his device to make phone calls, Mr.  
 8 Laning has used it for text messaging. Mr. Laning would not have purchased his mobile device had  
 9 he known that the Carrier IQ Software and related implementing or porting software was installed  
 10 and operating on his device, and taxing his device's battery, processor, and memory, as alleged  
 11 herein.

12 21. Plaintiff Clarissa Portales resides in Dallas, Texas. Plaintiff Portales purchased an  
 13 HTC EVO phone in 2010. Upon information and belief, Ms. Portales's mobile device came with  
 14 the Carrier IQ Software and implementing or porting software pre-installed. In addition to using  
 15 her device to make phone calls, Ms. Portales used it for web browsing and text messaging,  
 16 including accessing, inputting, and transmitting personal, private, confidential, and sensitive  
 17 information. Ms. Portales would not have purchased her mobile device had she known that the  
 18 Carrier IQ Software and related implementing or porting software was installed and operating on  
 19 her device, and taxing her device's battery, processor, and memory, as alleged herein.

20 22. Plaintiff Douglas White resides in Houston, Texas. Plaintiff White purchased a  
 21 Huawei Ascend II m865 mobile device in October 2011. Upon information and belief, Mr. White's  
 22 mobile device came with the Carrier IQ Software and implementing or porting software, pre-  
 23 installed. In addition to using his device to make phone calls Mr. White has used his mobile device  
 24 for web browsing and text messaging, including accessing, inputting, and transmitting personal,  
 25 private, confidential, and sensitive information. Mr. White would not have purchased his mobile  
 26 device had he known that the Carrier IQ Software and related implementing or porting software  
 27 was installed and operating on his device, and taxing his device's battery, processor, and memory,  
 28 as alleged herein.

1       23. Plaintiff Eric Thomas resides in New Braunfels, Texas. Plaintiff Thomas purchased  
 2 a Samsung Replenish mobile device in 2010. Upon information and belief, Mr. Thomas's mobile  
 3 device came with the Carrier IQ Software and implementing or porting software pre-installed. In  
 4 addition to using his device to make phone calls, Mr. Thomas has used his mobile device for web  
 5 browsing and text messaging, including accessing, inputting, and transmitting personal, private,  
 6 confidential, and sensitive information. Mr. Thomas would not have purchased his mobile device  
 7 had he known that the Carrier IQ Software and related implementing or porting software was  
 8 installed and operating on his device, and taxing his device's battery, processor, and memory, as  
 9 alleged herein.

10      24. Plaintiff Brian Sandstrom resides in San Francisco, California, but at pertinent times  
 11 to this matter, he resided in Seattle, Washington. Plaintiff Sandstrom purchased an HTC EVO  
 12 mobile device in 2010. Upon information and belief, Mr. Sandstrom's mobile device came with the  
 13 Carrier IQ Software and implementing or porting software pre-installed. In addition to using his  
 14 device to make phone calls, Mr. Sandstrom has used his mobile device for web browsing and text  
 15 messaging, including accessing, inputting, and transmitting personal, private, confidential, and  
 16 sensitive information. Mr. Sandstrom would not have purchased his mobile device had he known  
 17 that the Carrier IQ Software and related implementing or porting software was installed and  
 18 operating on his device, and taxing his device's battery, processor, and memory, as alleged herein.

19      25. Plaintiff Colleen Fischer resides in Janesville, Wisconsin. Plaintiff Fischer  
 20 purchased an LG LS670 Optimus S mobile device in 2011. Upon information and belief, Ms.  
 21 Fischer's mobile device came with the Carrier IQ Software and implementing or porting software  
 22 pre-installed. In addition to using her device to make phone calls, Ms. Fischer has used her mobile  
 23 device for web browsing and text messaging, including accessing, inputting, and transmitting  
 24 personal, private, confidential, and sensitive information. Ms. Fischer would not have purchased  
 25 her mobile device had she known that the Carrier IQ Software and related implementing or porting  
 26 software was installed and operating on her device, and taxing her device's battery, processor, and  
 27 memory, as alleged herein.

1                   **The defendants**

2         26. Defendant Carrier IQ, Inc. (“Carrier IQ” or “CIQ”) is a Delaware corporation  
 3 headquartered in Mountain View, California, with additional present or former offices in Chicago,  
 4 Boston, London (U.K.), and Kuala Lumpur (Malaysia). Carrier IQ is the designer, author,  
 5 programmer, and vendor of the IQ Agent and of the guide or template for the related implementing  
 6 or porting software known as the CIQ Interface. Furthermore, as discussed herein, Carrier IQ  
 7 remains heavily involved with Carrier IQ Software after a sale or license, including with respect to  
 8 its installation on mobile devices, which it works with the defendant manufacturers to effect, and  
 9 with the software’s activation, operation, and data collection and transmittals.

10       27. Defendant HTC America, Inc. (“HTC America”) is a Washington corporation with  
 11 its principal place of business in Bellevue, Washington. HTC America builds and sells mobile  
 12 devices throughout the United States that are based on the Android mobile operating system  
 13 (“Android OS”).

14       28. Defendant HTC Corporation (“HTC Corp.”) is a Taiwanese corporation and mobile  
 15 device manufacturer located in Taoyuan, Taiwan. It also is the parent to defendant HTC America,  
 16 Inc. HTC Corp. builds and sells mobile devices throughout the United States that are based on the  
 17 Android OS.

18       29. HTC America and HTC Corp. are collectively referred to as “HTC.” HTC is the  
 19 author and programmer of the CIQ Interface software used on HTC mobile devices referred to  
 20 herein. Upon information and belief, HTC installed the Carrier IQ Software and CIQ Interface  
 21 software on all the HTC mobile device models referenced herein. It is not yet known if any, or how  
 22 many, other HTC mobile device models bear or bore the software at issue.

23       30. Defendant Huawei Device USA, Inc. (“Huawei”) is a Texas corporation with its  
 24 principal place of business in Plano, Texas. Huawei builds and sells mobile devices throughout the  
 25 United States that are based on the Android OS. Upon information and belief, CIQ Interface  
 26 software was deployed on the Huawei devices at issue, and that Huawei was the author and  
 27 programmer of that software. Also, upon information and belief, Huawei installed the Carrier IQ  
 28 Software and CIQ Interface software on all the Huawei mobile device models referenced herein. It

1 is not yet known if any, or how many, other Huawei mobile device models bear or bore the  
 2 software at issue.

3       31. Defendant LG Electronics MobileComm U.S.A., Inc. (“LG MobileComm”) is a  
 4 California corporation with its principal place of business in San Diego, California. LG  
 5 MobileComm builds and sells mobile devices throughout the United States that are based on the  
 6 Android OS.

7       32. Defendant LG Electronics, Inc. (“LG Electronics”) is a South Korean corporation  
 8 with its principal place of business in Seoul, South Korea. LG Electronics builds and sells mobile  
 9 devices throughout the United States that are based on the Android OS.

10      33. LG MobileComm and LG Electronics are collectively referred to as “LG.” Upon  
 11 information and belief, CIQ Interface software was deployed on the LG devices at issue, and that  
 12 LG was the author and programmer of that software. Also, upon information and belief, LG  
 13 installed the Carrier IQ Software and CIQ Interface software on all the LG mobile device models  
 14 referenced herein. It is not yet known if any, or how many, other LG mobile device models bear or  
 15 bore the software at issue.

16      34. Defendant Motorola Mobility LLC (“Motorola”) is a Delaware limited liability  
 17 company with its principal place of business in Libertyville, Illinois. Motorola was formerly known  
 18 as Motorola Mobility, Inc. Motorola builds and sells mobile devices throughout the United States  
 19 that are based on the Android OS. Upon information and belief, CIQ Interface software was  
 20 deployed on the Motorola devices at issue, and that Motorola was the author and programmer of  
 21 that software. Also, upon information and belief, Motorola installed the Carrier IQ Software and  
 22 CIQ Interface software on all the Motorola mobile device models referenced herein. It is not yet  
 23 known if any, or how many, other Motorola mobile device models bear or bore the software at  
 24 issue.

25      35. Defendant Pantech Wireless, Inc. (“Pantech”) is a Georgia corporation with its  
 26 principal place of business in Atlanta, Georgia. Pantech builds and sells mobile devices throughout  
 27 the United States that are based on the Android OS. Upon information and belief, it is more likely  
 28 than not that CIQ Interface software was deployed on the Pantech devices at issue, and that

1 Pantech was the author and programmer of that software. Also, upon information and belief,  
 2 Pantech installed the Carrier IQ Software and CIQ Interface software on all the Pantech mobile  
 3 device models referenced herein. It is not yet known if any, or how many, other Pantech mobile  
 4 device models bear or bore the software at issue.

5       36. Defendant Samsung Telecommunications America, Inc. (“STA”) is a Delaware  
 6 corporation with its principal place of business in Richardson, Texas. STA builds and sells mobile  
 7 devices throughout the United States that are based on the Android OS.

8       37. Defendant Samsung Electronics Co., Ltd. (“SEC”) is a South Korean company with  
 9 its principal place of business at 1320-10, Seocho 2-dong, Seocho-gu, Seoul 137-857, South Korea.  
 10 SEC has offices within the United States and California and sells its products throughout the  
 11 United States. SEC builds and sells mobile devices throughout the United States that are based on  
 12 the Android OS.

13       38. STA and SEC are collectively referred to as “Samsung.” Upon information and  
 14 belief, CIQ Interface software was deployed on the Samsung devices at issue, and that Samsung  
 15 was the author and programmer of that software. Also, upon information and belief, Samsung  
 16 installed the Carrier IQ Software and CIQ Interface software on all the Samsung mobile device  
 17 models referenced herein. It is not yet known if any, or how many, other Samsung mobile device  
 18 models bear or bore the software at issue.

19       39. Collectively, HTC, Huawei, LG, Motorola, Pantech, and Samsung are referred to as  
 20 the “Device Manufacturers.”

#### 21                          IV. FACTUAL BACKGROUND

##### 22                          A. Revelations and Deep Concerns Regarding Carrier IQ Software

23       40. In late November 2011 news broke widely that a software product known as Carrier  
 24 IQ, ostensibly a network diagnostics tool, was installed on, and intercepting communications,  
 25 content, and data on, millions of mobile devices, all without the knowledge of the vast majority of  
 26 consumers. At that time, the Carrier IQ website, <http://www.carrieriq.com>, included a rolling tally  
 27 showing that its software was installed on over 141,000,000 mobile devices worldwide. Consumers  
 28 did not know that their mobile devices bore this software because it was deeply hidden; they had

1 no notice that it was operating in the background, and they had no way to remove the software or to  
 2 opt-out of its functions.

3       41.     Earlier in November 2011, an independent security and privacy researcher, Trevor  
 4 Eckhart, had published on his website, <http://www.androidsecuritytest.com>, the results of work he  
 5 had done to understand the Carrier IQ Software once he discovered it running on his Android OS  
 6 HTC mobile device. (Mr. Eckhart also credited a member of the Android developer community,  
 7 k0nane, for k0nane's earlier detective work on Samsung devices bearing Carrier IQ Software.) Mr.  
 8 Eckhart's work included studying training materials and other descriptive materials available  
 9 publicly on Carrier IQ's website and elsewhere, examination of evidence of the software hidden  
 10 deeply on his device, and examination of records of software activities left on the system log, or  
 11 so-called logcat log - part of the Android OS logging system - of his device. Regular users could  
 12 not have examined evidence of Carrier IQ's workings and activities on their devices even if they  
 13 knew that the software was there; such examination requires technical skill much greater than that  
 14 possessed by most consumers, or it requires rooting a device, which not only requires great  
 15 technical skill, but voids warranties as well.

16       42.     Carrier IQ reacted strongly to Mr. Eckhart's publication of his work, as evidenced  
 17 by the cease-and-desist demand letter it sent him on or about November 16, 2011. In this letter, a  
 18 copy of which is attached as Exhibit A, Carrier IQ took extreme exception to the characterizations  
 19 made about its product on Mr. Eckhart's website, and it accused him of copyright infringement for  
 20 using its publicly available materials to illustrate his findings. It threatened to sue him if he did not  
 21 take down these materials from his website, and indeed, if he did not remove all references to  
 22 Carrier IQ from it. Carrier IQ even provided him with text that it demanded he release to the press  
 23 under his own name, whereby he would apologize and retract his characterizations of the software  
 24 and its functions—including the characterization that Carrier IQ is rootkit software, *i.e.*, stealthy  
 25 software designed to hide its processes from normal means of detection and to enable continued  
 26 privileged access to a computer device.

27       43.     Mr. Eckhart undertook a two-pronged response to Carrier IQ's letter. One response  
 28 was to contact the Electronic Frontier Foundation ("EFF") for legal assistance in responding to

1 Carrier IQ's threats. Another response was to redouble his efforts to understand the Carrier IQ  
 2 Software and to demonstrate that the installation on his own device was doing far more than was  
 3 necessary for network diagnostics. For example, one of the statements that Carrier IQ demanded he  
 4 make was to retract his observation that the software was, in Carrier IQ's words, "recording  
 5 keystrokes."

6       44. By letter dated November 21, 2011, EFF counsel responded to Carrier IQ on Mr.  
 7 Eckhart's behalf. A copy of that letter is attached as Exhibit B. Citing the fair use doctrine and  
 8 other pertinent law and facts, counsel rebutted Carrier IQ's claims, stated that Mr. Eckhart was  
 9 declining to accede to its demands, and demanded that Carrier IQ withdraw in writing its  
 10 allegations regarding Mr. Eckhart and his work.

11       45. On November 23, 2011, Carrier IQ's CEO wrote a letter to EFF counsel by which  
 12 Carrier IQ withdrew the threats it had made to Mr. Eckhart and stated that it was "deeply sorry for  
 13 any concern or trouble" that its previous letter may have caused him. A copy of this letter is  
 14 attached as Exhibit C.

15       46. A few days later, Mr. Eckhart published Part 2 of his work regarding Carrier IQ  
 16 Software, both via his website and also via a 17 minute video released on November 28, 2011, on  
 17 YouTube.<sup>3</sup> In these follow-up publications, Mr. Eckhart expanded on his previous observations  
 18 regarding Carrier IQ and its workings, and he demonstrated visually that indeed, Carrier IQ was  
 19 intercepting communications and a significant amount of data and content, including keystrokes.  
 20 He showed that the software was intercepting incoming SMS text messages. He also showed that  
 21 the software was intercepting outgoing web queries and search terms, including those that should  
 22 have been encrypted, given that they were sent via the HTTPS protocol. Worse, even when Mr.  
 23 Eckhart was using his phone solely over Wi-Fi, rather than on a cellular network, he showed that  
 24 Carrier IQ Software was intercepting keystrokes and content, including outgoing SMS text  
 25 messages and HTTPS transmittals (carrying search terms), in unencrypted, human-readable form.  
 26 He also showed that on his installation, the data and content intercepted as part of Carrier IQ

---

27       <sup>3</sup> [http://www.youtube.com/watch?v=T17XQI\\_AYNo](http://www.youtube.com/watch?v=T17XQI_AYNo) (last accessed June 23, 2014). As of the date  
 28 of this filing, the video had been viewed over 2.177 million times.

1 processes, including (a) HTTPS strings (carrying search terms), such as those created in HTTPS  
 2 Google searches or HTTPS log-ins to PayPal, and (b) the content of SMS text messages, were  
 3 being copied in unencrypted, human-readable text to his device's Android system log(s) (which  
 4 sometimes are referred to as logcat logs).

5       47. Following publication of Part 2 of Mr. Eckhart's report, the mainstream press joined  
 6 the technical press in reporting on Carrier IQ Software and the revelations about its widespread,  
 7 hidden deployment and workings. Within hours and in the following days, consumers expressed  
 8 deep concern about the privacy and security violations surrounding Carrier IQ. Among their  
 9 comments:

10      a. I have to say . . . this is insanity!! If companies were trying to obtain  
 11 knowledge about "the user's experience" they wouldnt [sic] need to know every  
 12 single word that is typed into SMS or the Web, rather just that we are using text  
 13 messages or the web. They have gone TOO FAR by going into peoples personal  
 14 data, without concent [sic]! There must be a way to prosecute! We as users didnt  
 15 [sic] AGREE to this , and we should be able to get rid of it! It is a VIOLATION OF  
 16 PRIVACY and action needs to be taken!

17      b. By reporting the private numbers called by an end user, CIQ has not only  
 18 violated the privacy of the user but of the call recipient. Pretend you are a patient  
 19 with a socially embarrassing [sic] condition and your doctor calls you on his HTC or  
 20 Samsung... they know you were called. This is actually a violation of HIPPA. You  
 21 never signed a consent for disclosure of any medical information. If he or she  
 22 replied with a text, they now know what your condition is and what treatment has  
 23 been discussed. Does that make you feel warm and fuzzy? This is a major lawsuit...

24      c. All I want is a phone that can be with me for medical emergencies. Why do  
 25 they have to data mine everything I do without my permission? The most  
 26 frightening part of this is that they have disabled the security when you go to an  
 27 https site. Not a problem for me since the phone is just a phone in my useage [sic],  
 28 but it is serious for those who have bought into using their phone for everything  
 from banking to websurfing to scanning tags in stores for more information on a  
 product.

29      d. The Carrier I.Q. statement about using the app to get informaton [sic] on  
 30 how the product works sounds like total crap - to me is [sic] is spying on customers  
 31 so that the information can be used in sales of products current and possibly in the  
 32 future. No one has a right to know what sites you visit. And I think it is a real  
 33 violation of trust to have the app installed and not making consumers aware of it and  
 34 what it does, and how to shut the damned thing off. I don't like anyone tracking my  
 35 movements because I don't trust their reasons for doing it will always be legitimate  
 36 and in my personal interest.

37      e. Isn't this wireless tapping in it's [sic] most malicious form inasmuch the  
 38 user [sic] is not aware that he is being hacked by Current IQ? Common [sic]  
 39 people this has to end. We are all sheep being led to the slaughter sublimely and the  
 40 perpetrators [sic] are reaping \$ millions from our letting them get away with it. It's

1 time to kick these companies off of our phones or have the ability to disable all  
 2 these wireless tapping programs embedded surreptitiously [sic] on our phones and  
 computers.

3 f. I'm pretty sure there is some form of legal ramifications involved with this....  
 4 this is DEFINITELY an invasion of privacy for those who did not approve the app  
 on their phones. Super shady business going on here.

5 'Why is this not opt-in and why is it so hard to fully remove?' Eckhart wrote at the  
 end of the video.'

6 Why exactly ----- ? ? ? This is creepy.

7 g. Carrier IQ showed \*their\* colors when the first thing they tried to do was  
 8 silence the security researcher who uncovered their software by filing a SLAPP  
 9 lawsuit against him (since withdrawn after a stinging rebuke from the EFF). This  
 company should be prosecuted for violation of US anti-wiretap laws. And carriers  
 10 should drop them like the poisonous hot potato they are.

11 h. Even without this IQ spyware, mobile phones are effectively tracking  
 12 devices. But this latest discovery is ten times worse. This has to be highly illegal.  
 Remember how British Telecom at first issues denials that their Phorm [sic] product  
 13 was tracking web users, but then it was judged to be illegal. We need class-action  
 law suits [sic] prosecute the phone manufacturers and the makers of this rootkit.

14 48. Lawmakers expressed deep concerns, too. On November 30, 2011, U.S. Sen. Al  
 15 Franken sent a letter to Carrier IQ, seeking answers to serious questions regarding the deployment,  
 16 functions, and workings of its software. On December 1, 2011, Sen. Franken followed up by  
 17 sending letters to mobile device manufacturers HTC, Motorola, and Samsung, and to wireless  
 18 carriers AT&T, Sprint, and T-Mobile as well, seeking answers to the same sort of questions he had  
 put to Carrier IQ.

19 49. Once this security flaw was identified, the Department of Homeland Security  
 20 ("DHS") also issued a directive on July 23, 2013, instructing police, fire, EMS, and security  
 21 personnel to install an application that could "detect and remove the malicious software." Roll Call  
 22 Release, Threats to Mobile Devices Using the Android Operating System  
 23 <http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf> (last visited June 22, 2014). DHS  
 24 noted that the Carrier IQ software was a rootkit that "[l]ogs the user's locations, keystrokes, and  
 25 passwords without the user's knowledge." *Id.*

1           50. Shortly thereafter, consumers filed the first proposed class-action suits against  
 2 Carrier IQ and mobile device manufacturers. Many more would follow, until about 70 were filed  
 3 all around the country.

4           **B. Carrier IQ Software as Deployed**

5           **1. The enormous number of affected devices**

6           51. The Device Manufacturers, in conjunction with Carrier IQ, have installed the  
 7 Carrier IQ Software on millions of mobile devices, without consumers' knowledge, and without  
 8 offering ways to delete the software or to opt-out of its functions, including those complained of  
 9 herein.

10          52. The responses by mobile device manufacturers to Sen. Franken's late-November  
 11 and early-December 2011 letters confirmed how widespread the deployment of Carrier IQ  
 12 Software is, or was at relevant times, on some of the nation's most popular mobile devices.

13          53. According to AT&T's December 14, 2011 letter to Sen. Franken, "CIQ software  
 14 (including versions integrated on the device and downloaded with AT&T's MTS application [the  
 15 latter being a voluntary application download]) is resident on about 1% of the devices on AT&T's  
 16 wireless network, or approximately 900,000 devices, with about 575,000 of those collecting and  
 17 reporting wireless and service performance information to AT&T." AT&T also stated that the  
 18 software was "integrated and active on eleven AT&T wireless consumer devices: Pantech Pursuit  
 19 II, Pantech Breeze 3, Pantech P5000 (Link 2), Pantech Pocket, Sierra Wireless Shockwave, LG  
 20 Thrill, ZTE Avail, ZTE Z331, SEMC Xperia Play, Motorola Atrix 2, and Motorola Bravo." AT&T  
 21 indicated further that the software "also is embedded on the HTC Vivid, LG Nitro and Samsung  
 22 Skyrocket devices, but has not been activated due to the potential for the software agent to interfere  
 23 with the performance of those devices." (Discovery will help the plaintiffs to understand this latter  
 24 statement as to the behavior of the embedded but purportedly not "activated" software on the  
 25 referenced devices.)

26          54. Sprint indicated in its December 13, 2011 response to Sen. Franken that "[t]o the  
 27 best of [its] knowledge, there are approximately 26 million active Sprint devices that have Carrier  
 28 IQ Software installed." It indicated that it "'tasks' (queries information about) a fraction of those

1 devices at any one time (a maximum of 1.3 million) for diagnostic needs” and a subset of those,  
 2 “approximately 30,000 devices,” for “research specific problems . . . .” It stated that the software is  
 3 installed “on a variety of Sprint devices, including mobile handsets and tablets. Various Sprint-  
 4 offered devices manufactured by the following manufacturers have Carrier IQ Software installed:  
 5 Audiovox, Franklin, HTC, Huawei, Kyocera, LG, Motorola, Novatel, Palmone, Samsung, Sanyo,  
 6 and Sierra Wireless.”

7       55. According to press reports and certain plaintiffs, Sprint began removing the Carrier  
 8 IQ Software from mobile devices used on its network via over-the-air (*i.e.*, over the cellular  
 9 network) updates beginning in January 2012. Plaintiffs presently do not know if the software has  
 10 been removed from all affected mobile devices operating on the Sprint network (though it is likely  
 11 that the software still resides on some consumers’ devices, including those belonging to consumers  
 12 who were no longer Sprint customers, and who therefore were unable to connect to Sprint’s  
 13 cellular network, at the time of the over-the-air updates), nor do plaintiffs know if Sprint has re-  
 14 deployed any Carrier IQ Software on any devices operating on its network. Furthermore, it is not  
 15 presently known with certainty if the reported removal effected removal of the CIQ Interface  
 16 software or only the IQ Agent software.

17       56. T-Mobile responded to Sen. Franken on December 20, 2011, and indicated that as of  
 18 that date, “approximately 450,000 T-Mobile customers use devices that contain Carrier IQ’s  
 19 diagnostic software.” It stated that it “currently uses Carrier IQ’s diagnostic software on the  
 20 following devices: HTC Amaze 4G, Samsung Galaxy S II, Samsung Exhibit II 4G, T-Mobile  
 21 MyTouch by LG, T-Mobile MyTouch Q by LG, LG DoublePlay, BlackBerry 9900, BlackBerry  
 22 9360, [and the] BlackBerry 9810.”

23       57. As for HTC, it advised in its letter to Sen. Franken dated December 14, 2011, that  
 24 “based on figures from wireless service providers, approximately 6.3 million HTC devices using  
 25 the Carrier IQ Software are active devices.” It stated that “[t]he Carrier IQ Software was first  
 26 integrated on the Hero, which became available to customers through Sprint on October 2009.  
 27 Other HTC devices that use the integrated Carrier IQ Software and the date of their availability in  
 28 the U.S. market [include]: Snap (Sprint)—June 2009, Touch Pro 2 (Sprint)—September 2009,

1 Hero (Sprint)—October 2009, Evo 4G (Sprint)—June 2010, Evo Shift 4G (Sprint)—January 2011,  
 2 Evo 3D (Sprint)—June 2011, Evo Design (Sprint)—October 2011, Amaze 4G (T-Mobile)—  
 3 October 2011, [and the] Vivid (AT&T)—November 2011.”

4       58. Samsung, in its September 14, 2011 letter to Sen. Franken wrote that “STA  
 5 [Samsung Telecommunications America, LLC] has sold to carriers (and their distributors and  
 6 agents) serving the U.S. market approximately 25 million total cell phones that were pre-installed  
 7 with Carrier IQ Software.” It indicated that Carrier IQ Software was installed on the “following  
 8 cell phones”—Sprint: “SPH-Z400, SPH-M800, SPH-M220, SPH-M540, SPH-M630, SPH-M320,  
 9 SPH-M810, SPH-M550, SPH-M240, SPH-M560, SPH-M330, SPH-M850, SPH-I350, SPH-M900,  
 10 SPH-M350, SPH-M360, SPH-M570, SPH-D700, SPH-M910, SPH-M920, SPH-P100, SPH-M260,  
 11 SPH-M380, SPH-M820, SPH-M580, SPH-D600, SPH-M930, [and the] SPH-D710”; T-Mobile:  
 12 “T989 [and the] T679”; Cricket: “SCH-R500, SCH-R631, SCH-R261, SCH-R380”; and AT&T:  
 13 “SGH-i727.”

14       59. To date, plaintiffs have been unable to obtain a copy of Motorola’s response to Sen.  
 15 Franken’s December 1, 2011 letter, but press reports dated December 21, 2011 indicate that  
 16 Motorola stated by letter that it had installed the Carrier IQ Software on four models: the Admiral,  
 17 Titanium, Bravo and Atrix 2 “at the request of its carrier partners, AT&T and Sprint.” According to  
 18 a press report, Motorola also stated that “[a]t the end of the third-quarter of 2011, [it had] sold a  
 19 total of approximately 145,000 units of these models to [its] wireless carrier partners.”

20       60. It is believed, and therefore alleged, that the Carrier IQ Software is or was  
 21 previously installed on other mobile devices sold in the American market. Discovery should reveal  
 22 these other makes and models of affected devices.

23       **2. Carrier IQ Software’s interception and transmittal of private communications  
 24 and content**

25       61. The defendants - Carrier IQ and the Device Manufacturers - designed, authored,  
 26 programmed, and installed the Carrier IQ Software on millions of consumers’ mobile devices.  
 27 They also are the cause of its workings as complained of by the plaintiffs. Though the defendants  
 28 contend that all of the plaintiffs’ complaints are properly directed to the wireless carriers, in fact,

1 the carriers say they never asked for or sought the private communications and content that the  
 2 Carrier IQ Software nevertheless intercepted and transmitted.

3       62. Carrier IQ designed, authored, programmed, and caused the installation and  
 4 activation of the Carrier IQ Software, including the so-called IQ Agent, on the devices at issue in  
 5 this case. Carrier IQ also designed, authored, and provided guides to the Device Manufacturers for  
 6 designing, authoring, programming, installing, and activating the CIQ Interface in deployments  
 7 done by way of the so-called “embedded” method of installation. (*See, e.g.,*  
 8 <http://www.carrieriq.com/documents/understanding-carrier-iq-technology/6461/> (linked document  
 9 at 6) (last accessed June 22, 2014).) Additionally, as part of its business model and as a function of  
 10 the way its software is programmed, Carrier IQ can and does cause uploads of data collected on  
 11 mobile devices either to its own servers or directly to the servers of its customers. . (*E.g., id.*  
 12 (linked document at 11-13).)

13       63. The CIQ Interface is a wrapping or porting layer of code designed to see, recognize,  
 14 and intercept a host of data and content, including SMS text message content and URLs containing  
 15 search terms, user names, and passwords, among the other content described herein, and to send  
 16 that material down to the IQ Agent for further processing and possible transmittals. (*E.g., id.*  
 17 (linked document at 6).) Once the Device Manufacturers design and program the CIQ Interface  
 18 with Carrier IQ’s aid, the Device Manufacturers install it, as well as the IQ Agent - collectively,  
 19 “the Carrier IQ Software” - on affected devices. (*See, e.g., id.*) Thus installed, the Carrier IQ  
 20 Software is able to, and does, intercept not only benign network diagnostic data, but also personal,  
 21 private, confidential, and sensitive communications and content from the mobile devices on which  
 22 it is installed. The defendants, having designed, authored, programmed, and installed both  
 23 components of the Carrier IQ Software, knew and intended what it would do.

24       64. The Carrier IQ Software operates in the background on affected mobile devices.  
 25 The typical user has no idea that it is running, nor can he or she turn it off, even as it stealthily  
 26 infringes on his or her privacy and taxes the device’s battery power, processor functions, and  
 27 system memory. (*See, e.g.,* “What is Carrier IQ? Why Should We Care?” (<http://forum.xda-developers.com/showpost.php?p=11763089>) (discussing “drain on batter life and performance”)

1 (last accessed June 22, 2014).) Also, unless they have advanced skills and are willing to root their  
 2 devices and void their warranties, users cannot delete the software (and even those who have that  
 3 skillset may be unable to remove it completely). Nor are device owners given the choice of opting  
 4 in or out of the software's functionality.

5       65. Though touted by defendants as a benign and simple service-improvement tool,  
 6 researchers including Mr. Eckhart have demonstrated (including in his 17 minute YouTube video),  
 7 and Carrier IQ admits, that the Carrier IQ Software intercepts data on mobile devices, including:  
 8 URLs, including those containing HTTP and HTTPS query strings embedded with information  
 9 such as search terms (which could reveal a consumer's health conditions, sexual orientation, or  
 10 other private information), user names, passwords, and granular, GPS-based geo-location  
 11 information (*even when a search is being conducted over Wi-Fi, rather than a mobile carrier's*  
 12 *cellular network*); granular, GPS-based geo-location information apart from that transmitted in  
 13 URLs; SMS text messages; telephone numbers dialed and attached to calls received; other dialer  
 14 keypad presses/keystrokes; and application purchases and uses, among other content. (*See, e.g.,*  
 15 <http://www.theverge.com/2011/12/5/2609662/carrier-iq-interview> (last accessed June 21, 2014)  
 16 (December 5, 2011 interview with Carrier IQ's then V.P. of Marketing, Andrew Coward) ("Q. So  
 17 we spent a while discussing SMS. What about HTTPS? We'd imagine that carriers might know  
 18 which webpages you're going to, since they're providing your internet connection, but HTTPS is  
 19 potentially a step beyond that. Sometimes you'll find website usernames, passwords and  
 20 geolocation embedded in an HTTPS URL, things that we wouldn't normally expect our carrier to  
 21 be looking at. A. It's a good question, *and it's important to highlight that kind of information is*  
 22 *available.*") (emphasis added).) The software intercepts these communications and content as part  
 23 of its calls on the operating system for so-called "metrics." According to Carrier IQ, most of this  
 24 information, with the exception of text message content and certain other types of keystrokes, is  
 25 intentionally stored in the device's RAM space on a rolling basis as a function of the software.<sup>4</sup>

---

26       4 Among Carrier IQ's products is one called IQ Experience Insight Manager. According to an  
 27 online information sheet, CIQ touts as a feature of its Insight Experience Manager the ability to  
 28 "[v]iew application and device feature usage, such as camera, music, messaging, browser and TV,"  
 among many other features and attributes. A copy of this information sheet is attached as Exhibit

1       66. Further, the Carrier IQ Software can and does capture and transmit device-specific  
 2 identifiers, such that the foregoing information can be mated with a specific device. (*See, e.g.*,  
 3 <http://www.carrieriq.com/documents/understanding-carrier-iq-technology/6461/> (linked document  
 4 at 3).)

5       67. The software also is designed to intercept text message content. Carrier IQ, as the  
 6 designer and author of the IQ Agent and of the guide for the CIQ Interface, acknowledges this, but  
 7 claims that that it is merely looking for certain codes that might be carried along with any message.  
 8 Even if that were true, the Carrier IQ software is intentionally designed to intercept all such  
 9 content, unbeknownst to consumers. (*See, e.g.*, [http://www.theregister.co.uk/2011/12/02/  
 carrier\\_iq\\_interview/?page=2](http://www.theregister.co.uk/2011/12/02/carrier_iq_interview/?page=2) (last accessed June 20, 2014) (December 2, 2011 interview with  
 11 Andrew Coward, in which he states, in part: “With the SMS [text message] one, there are control  
 12 messages that come to us through SMS. . . . So we look at SMS messages that come in . . . .”); *see  
 13 also* <http://www.theverge.com/2011/12/5/2609662/carrier-iq-interview> (December 5, 2011  
 14 interview with Andrew Coward) (“Q. Do you feel that’s happening now, that users have a good  
 15 understanding of what information is being collected? A. Well, given the press over the past week,  
 16 it suggests not . . . .”).) The Device Manufacturers also know this; they intentionally designed and  
 17 programmed the IQ Agent so that it would intercept this content. Thus, the defendants intentionally  
 18 intercept these electronic communications. Further, this functionality of the Carrier IQ Software -  
 19 its ability to intercept a wealth of data and private content - is what enabled text and other content  
 20 to be logged in the affected devices’ system logs, as Mr. Eckhart discussed in Part 2 of his analysis  
 21 and in his 17 minute YouTube video. Without their interception by the Carrier IQ software, text  
 22 message and other content could not have been logged and sent off the devices to Google, HTC,  
 23 and perhaps application developers and other third-parties.

24       68. “Profiles” are another aspect of the Carrier IQ Software experience. Via Profiles,  
 25 CIQ customers, typically wireless carriers but sometimes device manufacturers, specify which data  
 26 they want from that assembled pursuant to the above-referenced metrics. At designated times, or as

---

27 D. It is unknown presently whether this product was installed on any of the prospective class  
 28 members’ devices.

1 requested, the Profile-specified data is transmitted from the mobile device to the requester. But it is  
 2 important to note that the plaintiffs' wireless carriers deny ever seeking information such as  
 3 Internet search terms or text message or other private communications and content, whether by  
 4 way of Profiles or otherwise. So the defendants may not point to the carriers as the cause of the  
 5 interception or transmittal of such communications and content.

6       69.     The consequences of the Carrier IQ Software's interception of so much data can be  
 7 quite serious. In addition to the interceptions, capture, and transmittal of personal, private,  
 8 confidential, and sensitive data, which has nothing to do with network diagnostics or improvement,  
 9 deployment of the Carrier IQ Software has led directly to other grave breaches of privacy.

10      70.     First, due to a purported programming error, AT&T admits that the Carrier IQ  
 11 Software transmitted text message content to it. This admission, of course, underscores that the  
 12 Carrier IQ Software is intercepting and capturing that information in the manner specified in the  
 13 first instance. While both AT&T and Carrier IQ state that these transmittals were inadvertent; that  
 14 they were made in encrypted form and never decoded at the receiver end; and that they were made  
 15 only in limited circumstances, nonetheless, users' private text messages were intercepted and then  
 16 transmitted off their mobile devices without their knowledge and consent.

17      71.     Worse yet, with some deployments, including those on HTC mobile devices and  
 18 possibly on certain other devices as well, a copy of data and content intercepted for Carrier IQ  
 19 Software purposes was also sent in unencrypted, human-readable form to the system logs  
 20 (sometimes called the logcat logs) of affected devices. The capture of this information in human-  
 21 readable form, via so-called verbose logging, is starkly shown in Mr. Eckhart's YouTube video.

22      72.     Once there, as recognized by the FTC in its action against HTC, such data and  
 23 content - SMS text messages; material including URLs embedded with HTTP/HTTPS query  
 24 strings carrying web search terms, user names and passwords, and geo-location information;  
 25 telephone numbers; other keystrokes; and data related to application purchases and uses - lies  
 26 vulnerable to anyone with access to these logs, including those with malicious intent. Such  
 27 information should not be captured in these logs, yet as a direct consequence of the deployment of  
 28 the Carrier IQ Software, logging of such personal, private, confidential, and sensitive information

1 has occurred on a massive scale. (It is, after all, a copy of information intercepted for Carrier IQ  
 2 Software purposes that is being sent to the affected devices' logs.) Carrier IQ points the finger at  
 3 the handset manufacturers, in particular at HTC, as the cause of this logging. But others have  
 4 theorized that the switch for this sort of logging actually came from the CIQ Interface-related  
 5 guides that Carrier IQ provides to device manufacturers.

6       73. Still worse, because device and application crash reports call on information stored  
 7 in device logs, plaintiffs have confirmed via arbitration-related discovery in this matter that  
 8 personal, private, confidential, and sensitive communications in the form of complete text  
 9 messages, and possibly personal, private, confidential, and sensitive information captured in  
 10 HTTP/HTTPS strings such as web search terms, user names, and passwords; granular geo-location  
 11 data; telephone numbers; other keystrokes; and data related to application purchase uses, was  
 12 transmitted to Google, the author of the Android OS, as part of, or along with, crash reports.  
 13 Additionally, HTC has acknowledged the receipt of such content by way of its Tell HTC tool,  
 14 which draws on content stored in the device logs. And further, such content may have gone to  
 15 application developers who draw on device logs as a means of diagnosing application crashes (or  
 16 for other purposes), including via widely available software tools such as ACRA. (*See, e.g.*,  
 17 <https://github.com/ACRA/acra>; <https://github.com/ACRA/acralyzer/wiki/usermanual> (last accessed  
 18 June 22, 2014).) Again, these actions were the direct result of the deployment of the Carrier IQ  
 19 Software on these devices, which was carried out jointly by Carrier IQ and the Device  
 20 Manufacturers.

21       74. Finally, as Mr. Eckhart showed in his video, such activity is taking place on mobile  
 22 devices bearing the Carrier IQ Software even if the consumer is no longer a customer of a wireless  
 23 carrier. So long as the software remains on the mobile device, it is functioning and transmitting as  
 24 stated above (save for functions only relatable to cellular telephone service), even when the  
 25 consumer is using the device solely on his or her home Wi-Fi network. Indeed, Mr. Eckhart  
 26 showed a search query, including the search term, intercepted by the software (and logged to the  
 27 device logcat log). Mobile device owners were unaware of this functionality of their Carrier IQ  
 28 Software-bearing devices, and it is one more reason why they would not have purchased these

1 devices had they known they were bearing the Carrier IQ Software that operated in the manners  
 2 alleged.

3       **3. The FTC's investigation of, and actions against, HTC involving Carrier IQ  
 4 Software**

5       75. After the filing of the First Consolidated Amended Complaint in this matter, the  
 6 FTC began an investigation of HTC America, Inc. with regard to the Carrier IQ Software and  
 7 related privacy and security flaws in the mobile devices sold by HTC.

8       76. On February 22, 2013, HTC reached an Agreement Containing Consent Order with  
 9 the FTC concerning serious security flaws HTC introduced to its Android and Windows Mobile  
 10 smartphones. After public comment, the FTC issued a Final Decision and Order on July 2, 2013  
 11 (although the Final Decision and Order itself is dated June 25, 2013). In its press release on July 2,  
 12 2013, the FTC stated that HTC America, Inc. "failed to take reasonable steps to secure the software  
 13 it developed for its smartphones and tablet computers, introducing security flaws that placed  
 14 sensitive information about millions of consumers at risk." ("FTC Approves Final Order Settling  
 15 Charges Against HTC America, Inc.," <http://www.ftc.gov/news-events/press-releases/2013/07/ftc-approves-final-order-settling-charges-against-htc-america-inc> (last visited June 22, 2014).) The  
 16 settlement agreement required HTC to "develop and release software patches to fix vulnerabilities  
 17 in millions of the company's devices." (*Id.*) Further, the settlement agreement required HTC to  
 18 establish a comprehensive security program designed to address security risks during the  
 19 development of HTC devices and to undergo independent security assessments every other year for  
 20 the next 20 years." (*Id.*) Last, HTC was prohibited from "making any false or misleading  
 21 statements about the security and privacy of consumers' data on HTC devices."

22       77. In the Final Complaint, issued on June 25, 2013 in connection with the Final  
 23 Decision and Order, the FTC alleged as follows:

24       **INSECURE COMMUNICATIONS MECHANISMS**

25       13. HTC failed to use readily-available and documented secure communications  
 26 mechanisms in implementing logging applications on its devices, placing sensitive  
 27 information at risk. Logging applications collect information that can be used, for  
 28 example, to diagnose device or network problems. Because of the sensitivity of the  
 information, as described below, communications with logging applications should

1           be secure to ensure that only designated applications can access the information.  
 2           Secure communications mechanisms -- such as the Android inter-process  
 3           communication mechanisms expressly described in the Android developer guides,  
 4           or secure UNIX sockets – could have been used to ensure that only HTC-designated  
 5           applications could access the sensitive information collected by the logging  
 6           application. Instead of using one of these well-known, secure alternatives, HTC  
 7           implemented communication mechanisms (e.g., INET sockets) that could not be  
 8           restricted in a similar manner. Moreover, HTC failed to implement other, additional  
 9           security measures (e.g., data encryption) that could have secured these  
 10           communications mechanisms. Because the communications mechanisms were  
 11           insecure, any third-party application that could connect to the internet could  
 12           communicate with the logging applications on HTC devices and access a variety of  
 13           sensitive information and sensitive device functionality, as described below.

14           a.        **HTC Loggers.** Beginning in May 2010, HTC installed its customer  
 15           support and trouble-shooting tool HTC Loggers on approximately 12.5  
 16           million Android-based mobile devices. Because HTC Loggers could collect  
 17           sensitive information from various device logs, it was supposed to have been  
 18           accessible only to HTC and certain network operators, and only after the  
 19           user had consented to its use by manually entering a special code into the  
 20           mobile device. Moreover, the Android permission-based security model  
 21           normally requires a third-party application to obtain the user's consent  
 22           before accessing the device logs. Because HTC used an insecure  
 23           communications mechanism, however, both of these intended protections  
 24           were undermined, and any third-party application on the user's device that  
 25           could connect to the internet could exploit the vulnerability to communicate  
 26           with HTC Loggers without authorization and command it to collect and  
 27           transmit information from the device logs. This information could include,  
 28           but was not limited to, contents of text messages; last known location and a  
 limited history of GPS and network locations; a user's personal phone  
 number, phone numbers of contacts, and phone numbers of those who send  
 text messages to the user; dialed digits; web browsing and media viewing  
 history; International Mobile Equipment Identity ("IMEI") or Mobile  
 Equipment Identifier ("MEID"); and registered accounts such as Gmail and  
 Microsoft Exchange account user names.

29           b.        **Carrier IQ.** Beginning in 2009, HTC embedded Carrier IQ  
 30           diagnostics software on approximately 10.3 million Android-based  
 31           mobile devices and 330,000 Windows Mobile-based mobile devices at the  
 32           direction of network operators Sprint and AT&T, who used Carrier IQ to  
 33           collect a variety of information, described in subparagraph (i) below, from  
 34           user devices to analyze network and device problems. In order to embed  
 35           the Carrier IQ software on its mobile devices, HTC developed a "CIQ  
 36           Interface" that would pass the necessary information to the Carrier IQ  
 37           software. The information collected by the Carrier IQ software was  
 38           supposed to have been accessible only to the network operators, but because  
 39           HTC used an insecure communications mechanism, any third-party  
 40           application on the user's device that could connect to the internet could

**exploit the vulnerability to communicate with the CIQ Interface, allowing it to:**

- i. Intercept the sensitive information being collected by the Carrier IQ software. This information could include, but was not limited to, GPS-based location information; web browsing and media viewing history; the size and number of all text messages; the content of each incoming text message; the names of applications on the user's device; the numeric keys pressed by the user; and any other usage and device information specified for collection by certain network operators; and
  - ii. In the case of HTC's Android-based devices, perform potentially malicious actions, including, but not limited to, sending text messages without permission. As described in Paragraph 11, malware could exploit this vulnerability to perpetrate toll fraud. Moreover, in this case, the sent text messages would not appear in the user's outbox, making it impossible for the user to verify that unauthorized text messages had been sent from the device.

## DEBUG CODE

14. During the development of an application, developers may activate “debug code” in order to help test whether the application is functioning as intended. When developing its CIQ Interface for its Android-based devices, HTC activated debug code in order to test whether the CIQ Interface properly sent all of the information specified by the network operator. The debug code accomplished this by writing the information to a particular device log known as the Android system log, which could then be reviewed. However, HTC failed to deactivate the debug code before its devices shipped for sale to consumers. As a result of the active debug code, all information that the CIQ Interface sent to the Carrier IQ software from a consumer’s device, including the information specified in Paragraph 13(b)(i), was also written to the Android system log on the device. This information was supposed to have been accessible only to the network operators, never written to the system log. Because it ended up in the system log, this sensitive information was:

- a. **Accessible to any third-party application with permission to read the system log.** Although users may provide third-party applications with permission to read the system log for certain purposes -- for example, to trouble-shoot application crashes -- those applications never should have had access to all the **sensitive information, such as the contents of incoming text messages, that the Carrier IQ software was collecting.**
  - b. **Sent to HTC.** The **information in the system log** is sent to HTC when a user chooses to send HTC an error report through its “Tell HTC” error reporting tool, described in Paragraph 20. Accordingly, in some cases, HTC also received this sensitive information, including users’ GPS-based location information.

1           15. HTC could have detected its failure to deactivate the debug code in its CIQ  
 2           Interface had it had adequate processes and tools in place for reviewing and testing  
 3           the security of its software code.

4           (FTC Complaint, dated June 25, 2013,  
 5           [http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702\\_htccmpt.pdf](http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702_htccmpt.pdf) (emphasis  
 6           added) (last visited June 22, 2013) .)

7           78.       The FTC also noted that “HTC could have implemented readily-available, low-cost  
 8           measures to address these vulnerabilities – for example, adding a few lines of permission check  
 9           code when programming its pre-installed applications, or implementing its logging applications  
 10          with secure communications mechanisms. *Consumers had little, if any, reason to know their*  
 11          *information was at risk because of the vulnerabilities introduced by HTC.*” *Id.* (emphasis added).

12          79.       In the Complaint accompanying the Final Decision and Order, the FTC leveled  
 13          three Counts against HTC, as follows:

14           **HTC'S UNFAIR SECURITY PRACTICES**

15           (Count 1)

16          21. As set forth in Paragraph 7-18, HTC failed to employ reasonable and  
 17          appropriate security practices in the design and customization of the software on its  
 18          mobile devices. HTC's practices caused, or are likely to cause, substantial injury to  
 19          consumers that is not offset by countervailing benefits to consumers or competition  
 20          and is not reasonably avoidable by consumers. This practice was, and is, an unfair  
 21          act or practice.

22           **HTC'S DECEPTIVE ANDROID USER MANUALS**

23           (Count 2)

24          22. As described in Paragraph 19, HTC has represented, expressly or by implication,  
 25          that, through the Android permission-based security model, a user of an HTC  
 26          Android-based mobile device would be notified when a third-party application  
 27          required access to the user's personal information or to certain functions or settings  
 28          of the user's device before the user completes installation of the third-party  
 application.

29          23. In truth and in fact, in many instances, a user of an HTC Android-based mobile  
 30          device would not be notified when a third-party application required access to the  
 31          user's personal information or to certain functions or settings of the user's device  
 32          before the user completes installation of the third-party application. Due to the  
 33          security vulnerabilities described in Paragraphs 8-15, third-party applications could  
 34          access a variety of sensitive information and sensitive device functionality on HTC  
 35          Android-based mobile devices without notifying or obtaining consent from the user  
 36          before installation. Therefore, the representation set forth in Paragraph 22  
 37          constitutes a false or misleading representation.

1                   HTC'S DECEPTIVE TELL HTC USER INTERFACE  
 2                   (Count 3)

3                   24. As described in Paragraph 20, HTC has represented, expressly or by implication,  
 4                   that, if a user does not check the button marked "Add location data" when  
 5                   submitting an error report through the Tell HTC application, location data would not  
 6                   be sent to HTC with the user's error report.

7                   25. In truth and in fact, in some instances, if a user did not check the button marked  
 8                   "Add location data" when submitting an error report through the Tell HTC  
 9                   application, location data was nevertheless sent to HTC with the user's error report.  
 10                  Due to the security vulnerability described in Paragraph 14, in some instances, HTC  
 11                  collected the user's GPS-based location information through the Tell HTC error  
 12                  reporting tool even when the user had not checked the button marked "Add location  
 13                  data" in the Tell HTC user interface. Therefore, the representation set forth in  
 14                  Paragraph 24 constitutes a false or misleading representation.

15                  26. The acts and practices of respondent as alleged in this complaint **constitute  
 16                  unfair or deceptive acts or practices in or affecting commerce in violation of  
 17                  Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).**

18                  (FTC Complaint, dated June 25, 2013, [http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702\\_htccmpt.pdf](http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702_htccmpt.pdf) (emphasis added) (last visited June 22, 2013) .)

19                  80.        In summary, the FTC found that the IQ Agent had been embedded by HTC into  
 20                  10.3 million of its mobile devices running on the Android OS, and another 330,000 devices  
 21                  running Windows Mobile. To do this, HTC designed and installed CIQ Interface software,  
 22                  including a debug code that permitted HTC to test whether the IQ Agent was intercepting the  
 23                  information for which it was designed. This information included "GPS-based location  
 24                  information; web browsing and media viewing history; the size and number of all text messages;  
 25                  the content of each incoming text message; the names of applications on the user's device; the  
 26                  numeric keys pressed by the user; and any other usage and device information specified for  
 27                  collection by certain network operators."

28                  81.        While the FTC's investigation and findings focused in part on the security flaws  
 29                  caused by HTC's failure to implement basic security measures, the findings regarding what could  
 30                  be and what was intercepted by the IQ Agent are crucial, and include highly sensitive information.  
 31                  Not only does this reveal the information actually intercepted, but it reveals that the IQ Agent *was  
 32                  designed to intercept the content of text messages, keypresses, location information, web browsing*

1       *history, and other personal information.* Furthermore, as HTC implemented a debug code to test  
 2 the IQ Agent's capabilities with regard to intercepting and collecting this highly sensitive  
 3 information, HTC must have known of the IQ Agent's capabilities.

4           82.     In its Complaint, the FTC stated succinctly that "HTC's practices caused, or are  
 5 likely to cause, substantial injury to consumers that is not offset by countervailing benefits to  
 6 consumers or competition and is not reasonably avoidable by consumers. This practice was, and is,  
 7 an unfair act or practice."

8           **4.     Further comments on Carrier IQ Software**

9           83.     Others have decried the actions of Carrier IQ and the Device Manufacturers and  
 10 investigated the functionality of the Carrier IQ Software.

11          84.     For example, in a December 8, 2011 online Computerworld article by Jaikumar  
 12 Vijayan entitled "Google's Schmidt calls Carrier IQ software a keylogger," the Executive  
 13 Chairman of Google, Eric Schmidt, was quoted as saying at an "Internet freedom conference" in  
 14 the Netherlands "that Carrier IQ's software is a keylogger that 'actually does keep your  
 15 keystrokes.'" Mr. Schmidt also was quoted as stating, "We certainly don't work with them and we  
 16 certainly don't support it." In addition, he was quoted as saying, "'Android is an open platform, so  
 17 it's possible for people to build software that's actually not very good for you, and this appears to  
 18 be one.'" Google, of course, is the owner and publisher of the Android OS.

19          85.     Android developer Tim Schofield researched the presence of the Carrier IQ  
 20 Software on multiple Android smartphone platforms. He has noted that in addition to the privacy  
 21 issues, the embedded Carrier IQ Software necessarily degrades the performance of any device on  
 22 which it is installed. ([http://www.youtube.com/watch?v=legx3K\\_Ul\\_I](http://www.youtube.com/watch?v=legx3K_Ul_I) at 9:44 (last accessed June  
 23 22, 2014).) The Carrier IQ Software is always operating and cannot be turned off. It necessarily  
 24 uses system resources, thus slowing performance and decreasing battery life. (*Id.*) As a result,  
 25 because of the Carrier IQ Software, in addition to having their private communications intercepted,  
 26 plaintiffs and prospective class members are not getting the optimal performance of the mobile  
 27 devices they purchased, and which are marketed, in part, based on their speed, performance, and  
 28 battery life.

## **V. CLASS ALLEGATIONS**

86. With respect to their claims under the Federal Wiretap Act (Count I), plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and a proposed class consisting of:

All persons in the United States who owned or purchased HTC, Huawei, LG, Motorola, Pantech, and Samsung mobile devices on which Carrier IQ Software is or was embedded or preloaded.

Excluded from the proposed class are defendants; defendants' affiliates and subsidiaries; defendants' current or former employees, officers, directors, agents, and representatives; and the district judge or magistrate judge to whom this case is assigned, as well as those judges' immediate family members.

87. In addition, plaintiffs ask that the Court certify appropriate classes comprised of consumers residing in the states listed in Counts II, III, IV, and V below. In order to aid the Court with manageability, plaintiffs anticipate proposing subclasses based on the similarity of laws from among those states listed with respect to Counts II, III, IV, and V.

88. **Numerosity:** The exact number of the members of the proposed class is unknown and is not available to the plaintiffs at this time, but individual joinder in this case is impracticable. Based on defendant Carrier IQ's representation that its software is installed on over 140 million devices and the representations of the Device Manufacturers and wireless carriers as to the number of mobile devices bearing Carrier IQ Software, the number of class and sub-class members could reach into the millions.

89. **Commonality:** Numerous questions of law and fact are common to the claims of the plaintiffs and members of the proposed class. These include:

a. Whether Carrier IQ Software installed on plaintiffs' and proposed class members' mobile devices has intercepted, or intercepted and transmitted, plaintiffs' and proposed class members' SMS text message content; URL or other inputs, including HTTP and HTTPS query strings containing search terms and/or user names and passwords; other keystrokes; telephone numbers (whether those of others the consumer calls, those of persons who call the consumer, or of

1 the consumer himself or herself); granular geo-location information; application purchase and use  
 2 data; and other information, and whether it continues to do so.

3       b.      Whether plaintiffs' and proposed class members' SMS text message content; URL  
 4 or other inputs, including HTTP and HTTPS query strings; other keystrokes; telephone numbers  
 5 (whether those of others the consumer calls, those of persons who call the consumer, or of the  
 6 consumer himself or herself); granular geo-location information; application purchase and use data;  
 7 and other information has been sent to the device, system, or logcat logs of their mobile devices,  
 8 and whether all or any such information has been transmitted off their devices to Google, HTC, or  
 9 third-party application developers and vendors, or to any other person or entity.

10       c.     Whether CIQ has violated the Federal Wiretap Act by way of the acts and  
 11 omissions set forth in this complaint.

12       d.     Whether the Device Manufacturers have violated the Federal Wiretap Act.

13       e.     Whether CIQ and the Device Manufacturers have violated state privacy statutes by  
 14 way of the acts and omissions set forth in this complaint.

15       f.     Whether CIQ and the Device Manufacturers have violated state consumer protection  
 16 laws by way of the acts and omissions set forth in this complaint.

17       g.     Whether the Device Manufacturers have violated the Magnuson-Moss Warranty Act  
 18 by way of the acts and omissions set forth in this complaint.

19       h.     Whether the Device Manufacturers have breached their implied warranties of  
 20 merchantability by way of the acts and omissions set forth in this complaint, entitling plaintiffs to  
 21 damages.

22       i.     Whether CIQ and the Device Manufacturers have unlawfully profited from their  
 23 conduct, and whether they must disgorge or restore profits, or make refunds or partial refunds, to  
 24 the plaintiffs and members of the proposed class.

25       j.     Whether plaintiffs and members of the prospective class would have purchased their  
 26 mobile devices if they had known that Carrier IQ Software was installed on them.

27       k.     Whether plaintiffs and members of the proposed class are entitled to statutory and  
 28 other damages, compensatory damages, civil penalties, punitive or multiple damages, restitution,

1 declaratory relief, injunctive relief, or other equitable relief, and whether they are entitled to the  
 2 maximum relief that they seek.

3       **90. Typicality:** Plaintiffs' claims are typical of the claims of the members of the  
 4 proposed class. The factual and legal bases of defendants' liability to plaintiffs and other members  
 5 of the proposed class are the same and resulted in injury to plaintiffs and all of the other members  
 6 of the proposed class.

7       **91. Adequate representation:** Plaintiffs will represent and protect the interests of the  
 8 proposed class both fairly and adequately. They have retained counsel competent and experienced  
 9 in complex class-action litigation. Plaintiffs have no interests that are antagonistic to those of the  
 10 proposed class, and their interests do not conflict with the interests of the proposed class members  
 11 they seek to represent.

12       **92. Predominance and Superiority:** This proposed class action is appropriate for  
 13 certification. Class proceedings on these facts and this law are superior to all other available  
 14 methods for the fair and efficient adjudication of this controversy, given that joinder of all  
 15 members is impracticable. Even if members of the proposed class could sustain individual  
 16 litigation, that course would not be preferable to a class action because individual litigation would  
 17 increase the delay and expense to all parties due to the complex factual and legal controversies  
 18 present in this controversy. Here, the class action device will present far fewer management  
 19 difficulties, and it will provide the benefit of a single adjudication, economies of scale, and  
 20 comprehensive supervision by this Court. Further, uniformity of decisions will be assured.

## 21                   **VI. CLAIMS FOR RELIEF**

### 22                   **COUNT I** 23                   **VIOLATION OF THE FEDERAL WIRETAP ACT**

24                   (Against Carrier IQ and the Device Manufacturers)

- 25       93. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.  
 26       94. Plaintiffs bring this claim on their own behalf and on behalf of a proposed  
 27 nationwide class of owners of affected devices.

1           95. Defendants Carrier IQ and the Device Manufacturers, by way of their design,  
 2 authorship, programming, knowing and intentional installation, activation, and/or other  
 3 involvement with the Carrier IQ Software, as alleged herein, have intentionally intercepted,  
 4 endeavored to intercept, and/or procured others to intercept or endeavor to intercept, electronic  
 5 communications as described herein, in violation of 18 U.S.C. § 2511(1). *See* 18 U.S.C. §  
 6 2511(1)(a).

7           96. As a result of these violations of law, plaintiffs and the prospective class have  
 8 suffered harm and injury, including by way of the interception and transmission of private and  
 9 personal, confidential, and sensitive communications, content, and data as alleged herein, as well as  
 10 the degraded performance level of their devices (including diminished battery power and life,  
 11 together with diminished performance due to taxation of the devices' processors and memory  
 12 caused by the constant operation of the Carrier IQ Software).

13          97. Accordingly, defendants Carrier IQ and the Device Manufacturers are subject to  
 14 civil suit, and plaintiffs and the class are entitled to appropriate relief, including that set forth in 18  
 15 U.S.C. § 2520(b). 18 U.S.C. § 2520(a). Such appropriate relief includes "preliminary or other  
 16 equitable or declaratory relief as may be appropriate"; "damages" as described in the statute; and "a  
 17 reasonable attorney's fee and other litigation costs reasonably incurred." 18 U.S.C. § 2520(b). As  
 18 for damages, "the court may assess as damages whichever is the greater of—(A) the sum of the  
 19 actual damages suffered by the plaintiff and any profits made by the violator as a result of the  
 20 violation; or (B) statutory damages of whichever is the greater of \$100 a day for each day of  
 21 violation or \$10,000." 18 U.S.C. § 2520(c)(2).

22          98. Plaintiffs, on their own behalf and on behalf of the proposed class, seek all such  
 23 appropriate relief, including, but not limited to, the maximum amount of statutory damages as set  
 24 forth above.

25          99. Investigation regarding disclosures, including intentional disclosures, of the  
 26 communications, content, information, and data referenced herein, or the endeavoring to disclose,  
 27 intentionally or otherwise, the communications, content, information, and data referenced herein, is  
 28 ongoing. Such activity may be actionable hereunder.

**COUNT II**  
**VIOLATION OF STATE PRIVACY ACTS**

(Against Carrier IQ and the Device Manufacturers)

(On Behalf of Residents of the States of Arizona, California, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming, and on Behalf of All U.S. Residents Under Cal. Penal Code § 502)

100. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

101. Plaintiffs bring these claims on behalf of themselves and other owners of affected devices who reside in the states of Arizona, California, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming, and on behalf of all U.S. owners of affected devices under California Penal Code § 502.

102. By way of their actions as stated herein, which include their design, authorship, programming, knowing and intentional installation, and activation of, and their other involvement with, the Carrier IQ Software as alleged herein, as well as by way of their interceptions of communications and content including SMS text messages; URLs and other inputs containing HTTP and HTTPS strings embedded with confidential and sensitive material such as search terms, user names, and passwords; and dialer-pad keypresses, as well as the capture of granular geo-location information traceable to individual consumers by way of unique mobile device identifiers, defendants Carrier IQ and the Device Manufacturers have violated state privacy acts as set forth herein.

103. For example, defendants have violated California's Computer Crime Law, Cal. Penal Code §§ 502, *et seq.*

104. California Penal Code § 502 prohibits “tampering, interference, damage and unauthorized access to lawfully created computer data and computer systems.” A mobile device is

1 a “computer system” as defined in Cal. Penal Code § 502(b)(5) because it contains electronic  
 2 instructions, inputs and outputs data, and performs computerized functions including  
 3 communications and data storage and retrieval.

4       105. Defendants have violated California Penal Code § 502 by knowingly accessing,  
 5 copying, using, making use of, interfering, and/or altering plaintiffs’ and prospective class  
 6 members’ data such as URLs containing HTTP and HTTPS query strings embedded with  
 7 information including search terms, user names, passwords, and granular geo-location information;  
 8 granular geo-location information apart from that transmitted in URLs; text messages; telephone  
 9 numbers dialed and received; other keystrokes; and application purchases and uses. Defendants so  
 10 acted on a systematic and continuous basis.

11       106. Civil actions lie for violations of California Penal Code § 502. Cal. Penal Code §  
 12 502(e)(1). Defendants’ actions have caused damages to plaintiffs and the prospective class,  
 13 including by way of the consumption of battery power (indeed, following the removal of Carrier IQ  
 14 Software from various mobile devices, users report dramatically increased times between battery  
 15 charges) and system memory and processing resources which demonstrably affect performance of  
 16 their mobile devices. These damages are quantifiable and will be provable at trial. In addition,  
 17 plaintiffs and members of the prospective class will be entitled to recover their reasonable  
 18 attorneys’ fees pursuant to California Penal Code § 502(e)(2).

19       107. Furthermore, plaintiffs and the class are entitled to injunctive relief to prevent the  
 20 further interception or capture and transmittal of data such as URLs containing HTTP and HTTPS  
 21 query strings embedded with information such as search terms, user names, passwords, and geo-  
 22 location information; geo-location information apart from that transmitted in URLs; text messages;  
 23 telephone numbers dialed and received; other keystrokes; and information relating to application  
 24 purchases and uses. They also are entitled to injunctive and other equitable relief to remedy any  
 25 continuing copying of the foregoing information, as well as SMS text message content, to system  
 26 logs, which are being transmitted off-device to Google, to HTC, and possibly to third-party  
 27 application developers without authorizations, and the logging of which creates extreme  
 28 vulnerability to capture by deliberate means.

1           108. Damages and injunctive and other equitable relief are available to all plaintiffs and  
 2 members of the prospective class, wherever they may live in the United States. Cal. Penal Code §  
 3 502(j) (“For purposes of bringing a civil or a criminal action under this section, a person who  
 4 causes, by any means, the access of a computer, computer system, or computer network in one  
 5 jurisdiction from another jurisdiction is deemed to have personally accessed the computer,  
 6 computer system, or computer network in each jurisdiction.”).

7           109. In addition, by intercepting communications including URLs containing HTTP and  
 8 HTTPS query strings embedded with information such as search terms, user names, and  
 9 passwords; text messages; and other keystrokes; as well as by way of the other interceptions of  
 10 communications described herein, defendants have violated California Penal Code § 632.7. That  
 11 statute provides that “[e]very person who, without the consent of all parties to a communication,  
 12 intercepts or receives and intentionally records, or assists in the interception or reception and  
 13 intentional recordation of, a communication transmitted between two cellular radio telephones, a  
 14 cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and  
 15 a landline telephone, or a cordless telephone and a cellular radio telephone,” is punishable by fines,  
 16 imprisonment, or both. Cal. Penal Code § 632.7(a).

17           110. Defendants are liable in a civil action for violation of California Penal Code 632.7  
 18 by way of California Penal Code § 637.2. California Penal Code § 637.2 provides for the recovery  
 19 of \$5,000 or three times actual damages, whichever is greater. Cal. Penal Code § 637.2(a). In  
 20 addition, plaintiffs may seek to bring an action “to enjoin and restrain any violation of this chapter,  
 21 and may in the same action seek damages . . .” Cal. Penal Code § 637.2(a). Because it is likely  
 22 that statutory damages of \$5,000 will exceed three times their actual damages, plaintiffs, on behalf  
 23 of themselves and the prospective class, seek an award of \$5,000 for each violation of these laws.

24           111. In addition, pursuant to California Penal Code § 637.2, plaintiffs and the prospective  
 25 class are entitled to injunctive relief to prevent the admitted interception or capture and transmittal  
 26 of URLs containing HTTP and HTTPS query strings embedded with information such as search  
 27 terms, user names, and passwords; text messages; telephone numbers dialed and received; and  
 28 other keystrokes; and other communications as described herein. They also are entitled to

1 injunctive and other equitable relief to remedy any continuing copying of the foregoing  
 2 communications to device system, or logcat, logs, which have been, and in some instance possibly  
 3 are still being, transmitted off-device to Google, HTC, and possibly to third-party application  
 4 developers, and whose logging creates extreme vulnerability to capture by deliberate means.

5       112. Also, plaintiffs and the prospective class are entitled to recover their attorneys' fees  
 6 because by way of this lawsuit, they seek to enforce important rights affecting the public interest,  
 7 and because they otherwise satisfy the statutory requirements for an award of attorneys' fees. Cal.  
 8 Code of Civil Proc. § 1021.5.

9       113. As a result of defendants' actions as described above and herein, which descriptions  
 10 are incorporated here, plaintiffs and owners of affected devices who reside in states other than  
 11 California are likewise entitled to similar damages, including statutory damages, punitive damages  
 12 where available, and injunctive or other equitable relief, as well as attorneys' fees and costs, under  
 13 similar laws of their home states as follows:

14       a.      **Arizona.** Ariz. Rev. Stat. § 12-731 provides for the recovery in a civil action  
 15 of relief for violations of Ariz. Rev. Stat. § 13-3005(A)(1), which, in pertinent part,  
 16 provides that a person is guilty of a felony who, without consent, either intentionally  
 17 intercepts an electronic communication (*see* Ariz. Rev. Stat. § 13-3001(4)) or aids  
 18 or procures others to do so.

19           Defendants Carrier IQ and the Device Manufacturers, by way of their  
 20 programming, knowing and intentional installation, activation, and other  
 21 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 22 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 23 authorized, employed, or procured or permitted others to do so.

24           Accordingly, plaintiffs and the class are entitled under Ariz. Rev. Stat. § 12-  
 25 731 to "preliminary and other equitable or declaratory relief as may be appropriate,"  
 26 as well as damages "in an amount that is the greater of either" . . . "[s]tatutory  
 27 damages of one hundred dollars a day for each day of the violation" or "statutory  
 28 damages of ten thousand dollars." They also are entitled to punitive damages in this

1 case, as well as their “[r]easonable attorney fees and other reasonable costs of  
 2 litigation.”

3       **b. Connecticut.** Conn. Gen. Stat. § 54-41r provides for the recovery in a civil  
 4 action of relief for its violation. It provides in pertinent part that “[a]ny person  
 5 whose wire communication [*see* Conn. Gen. Stat. § 54-41a(1), defining “wire  
 6 communication” in such a manner as to encompass the communications here at  
 7 issue] is intercepted, disclosed, or used in violation of [the subject chapter or  
 8 sections] shall have a . . . civil cause of action against any person who intercepts,  
 9 discloses or sues, or procures another person to intercept, disclose or use, such  
 10 communication . . . .”

11              Defendants Carrier IQ and the Device Manufacturers, by way of their  
 12 programming, knowing and intentional installation, activation, and other  
 13 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 14 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 15 authorized, employed, or procured or permitted others to so do.

16              Accordingly, plaintiffs and the class are entitled under Conn. Gen. Stat. §  
 17 54-41r to recover from the defendants “actual damages but not less than liquidated  
 18 damages computed at the rate of one hundred dollars per day for each day of  
 19 violation or one thousand dollars, whichever is higher; punitive damages; and a  
 20 reasonable attorney’s fee and other litigation costs reasonably incurred.”

21       **c. Delaware.** 11 Del. Code § 2409 provides for the recovery in a civil action of  
 22 relief for violations of 11 Del. Code § 2402(a)(1)-(3), which, in pertinent part,  
 23 provides that no person shall “intentionally intercept, endeavor to intercept, or  
 24 procure any other person to intercept or endeavor to intercept any wire, oral or  
 25 electronic communication,” *see* 11 Del. Code § 2401(5), or intentionally disclose or  
 26 endeavor to disclose, or intentionally use or endeavor to use, electronic  
 27 communications intercepted in violation of the subject chapter.

1                   Defendants Carrier IQ and the Device Manufacturers, by way of their  
 2 programming, knowing and intentional installation, activation, and other  
 3 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 4 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 5 authorized, employed, or procured or permitted others to so do.

6                   Accordingly, plaintiffs and the class are entitled under 11 Del. Code § 2409  
 7 to their “actual damages, but not less than liquidated damages computed at the rate  
 8 of \$100 dollars a day for each day of the violation or \$1,000, whichever is higher;  
 9 “[p]unitive damages”; and a “reasonable attorney’s fee and other litigation costs  
 10 reasonably incurred.”

11                 d.       **Florida.** Fla. Stat. § 934.10 provides for the recovery in a civil action of  
 12 relief for violations of Fla. Stat. § 934.03(1)(a), which provides in pertinent part:

13                 (1) Except as otherwise specifically provided in this chapter,  
 14 any person who:

15                 (a) Intentionally intercepts, endeavors to intercept, or  
 16 procures any other person to intercept or endeavor to intercept any  
 wire, oral, or electronic communication;

17                 (b) Intentionally uses, endeavors to use, or procures any other  
 18 person to use or endeavor to use any electronic, mechanical, or other  
 device to intercept any oral communication when:

19                 1. Such device is affixed to, or otherwise transmits a signal  
 20 through, a wire, cable, or other like connection used in wire  
 21 communication; or

22                 2. Such device transmits communications by radio or  
 23 interferes with the transmission of such communication;

24                 (c) Intentionally discloses, or endeavors to disclose, to any  
 25 other person the contents of any wire, oral, or electronic  
 26 communication, knowing or having reason to know that the  
 information was obtained through the interception of a wire, oral, or  
 electronic communication in violation of this subsection;

27                 (d) Intentionally uses, or endeavors to use, the contents of any  
 28 wire, oral, or electronic communication, knowing or having reason to  
 know that the information was obtained through the interception of a

wire, oral, or electronic communication in violation of this subsection; or

(e) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2, paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation;

shall be punished as provided in subsection (4).

*See also* Fla. Stat. § 934.02(12) (defining "electronic communication").

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Fla. Stat. § 934.10 provides in pertinent part that:

(1) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of ss. 934.03-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any other person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including:

(a) Preliminary or equitable or declaratory relief as may be appropriate:

(b) Actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;

(c) Punitive damages; and

(d) A reasonable attorney's fee and other litigation costs reasonably incurred

1           Based on the allegations herein, plaintiffs and the class are entitled to  
 2 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 3 damages provided by the foregoing statute, including punitive damages; and a  
 4 reasonable attorney's fee and other litigation costs reasonably incurred.

5         e.      **Hawaii.** Haw. Rev. Stat. § 803-48 provides for the recovery in a civil action  
 6 of relief for violations of Haw. Rev. Stat. § 803-42(a)(1), which, in pertinent part,  
 7 provides:

8                 (a) Except as otherwise specifically provided in this part, any  
 9 person who:

10                 (1) Intentionally intercepts, endeavors to intercept, or procures any  
 11 other person to intercept or endeavor to intercept, any wire, oral, or  
 12 electronic communication;

13                 (2) Intentionally uses, endeavors to use, or procures any other person  
 14 to use or endeavor to use any electronic, mechanical, or other device  
 15 to intercept any wire, oral, or electronic communication when:

16                     (A) Such a device is affixed to, or otherwise transmits a signal  
 17 through, a wire, cable, or other similar connection used in wire  
 18 communication; or

19                     (B) Such a device transmits communications by radio, or interferes  
 20 with the transmission of such communication;

21                 (3) Intentionally discloses, or endeavors to disclose, to any other  
 22 person the contents of any wire, oral, or electronic communication,  
 23 knowing or having reason to know that the information was obtained  
 24 through the interception of a wire, oral, or electronic communication  
 25 in violation of this part;

26                 (4) Intentionally uses, or endeavors to use, the contents of any wire,  
 27 oral, or electronic communication, knowing or having reason to  
 28 know that the information was obtained through the interception of a  
 29 wire, oral, or electronic communication in violation of this part;

30                 (5)(A) Intentionally accesses without authorization a facility through  
 31 which an electronic communication service is provided; or

32                     (B) Intentionally exceeds an authorization to access that facility; and  
 33 thereby obtains, alters, or prevents authorized access to a wire or  
 34 electronic communication while it is in electronic storage;

(6) Intentionally discloses, or attempts to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by subsection (b)(1), (2), or (3), or section 803-44 or 803-46; and

(A) Either:

(i) Knowing or having reason to know that the information was obtained through the interception of the communication in connection with a criminal investigation; or

(ii) Having obtained or received the information in connection with a criminal investigation; and

(B) With the intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation[;]

(7) Intentionally installs or uses a pen register or a trap and trace device without first obtaining a court order; or

(8) Intentionally installs or uses a mobile tracking device without first obtaining a search warrant or other order authorizing the installation and use of such device, unless the device is installed by or with consent of the owner of the property on which the device is installed;

shall be guilty of a class C felony.

*See also* Haw. Rev. Stat. § 803-41 (defining “electronic communication”).

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Haw. Rev. Stat. § 803-48 provides:

Any person whose wire, oral, or electronic communication is accessed, intercepted, disclosed, or used in violation of this part shall (1) have a civil cause of action against any person who accesses, intercepts, discloses, or uses, or procures any other person to access, intercept, disclose, or use the communications, and (2) be entitled to recover from any such person:

1                             (A) The greater of (i) the sum of the actual damages suffered by the  
 2 plaintiff and any profits made by the violator as a result of the  
 3 violation, or (ii) statutory damages of the greater of \$100 a day for  
 4 each day of violation or \$10,000;

5                             (B) Punitive damages, where appropriate; and

6                             (C) A reasonable attorney's fee and other litigation costs reasonably  
 7 incurred.

8                             The aggrieved person may also seek and be awarded such  
 9 preliminary, and other equitable or declaratory relief as may be  
 10 appropriate. A good faith reliance on a court order shall constitute a  
 11 complete defense to any civil action brought under this part.

12                             Based on the allegations herein, plaintiffs and the class are entitled to  
 13 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 14 damages provided by the foregoing statute, including punitive damages; and a  
 15 reasonable attorney's fee and other litigation costs reasonably incurred.

16                         f.         **Idaho.** Idaho Code § 18-6709 provides for the recovery in a civil action of  
 17 relief for violations of Idaho Code § 18-6702(1)(a), (c), and (d), which, in pertinent  
 18 part, provides:

19                             (1) Except as otherwise specifically provided in this chapter,  
 20 any person shall be guilty of a felony and is punishable by  
 21 imprisonment in the state prison for a term not to exceed five (5)  
 22 years or by a fine not to exceed five thousand dollars (\$5,000), or by  
 23 both fine and imprisonment if that person:

24                             (a) Willfully intercepts, endeavors to intercept, or procures  
 25 any other person to intercept or endeavor to intercept any wire,  
 26 electronic or oral communication; or

27                             (b) Willfully uses, endeavors to use, or procures any other  
 28 person to use or endeavor to use any electronic, mechanical, or other  
 device to intercept any oral communication when:

1. Such device is affixed to, or otherwise transmits a signal  
 through, a wire, cable, or other like connection used in wire  
 communication; or

2. Such device transmits communications by radio or  
 interferes with the transmission of such communication; or

(c) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this subsection; or

(d) Willfully uses, or endeavors to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this subsection; or

(e) Intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, intercepted by means authorized by subsection (2)(b), (c), (f) or (g) of this section or by section 18-6708, Idaho Code, if that person:

(i) Knows or has reason to know that the information was obtained through the interception of such communication in connection with a criminal investigation; and

(ii) Has obtained or received the information in connection with a criminal investigation with the intent to improperly obstruct, impede or interfere with a duly authorized criminal investigation.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

**Idaho Code § 18-6709** provides in pertinent part:

Any person whose wire, electronic or oral communication is intercepted, disclosed, or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses, uses, or procures any other person to intercept, disclose, or use such communications, and shall be entitled to recover from any such person:

(a) Actual damages, but not less than liquidated damages computed at the rate of one hundred dollars (\$100) a day for each

1                   day of violation or one thousand dollars (\$1,000), whichever is  
 2                   higher;

3                   (b) Punitive damages; and

4                   (c) A reasonable attorney's fee and other litigation costs  
 5                   reasonably incurred.

6                   Based on the allegations herein, plaintiffs and the class are entitled to the  
 7                   maximum damages provided by the foregoing statute, including punitive damages;  
 8                   and a reasonable attorney's fee and other litigation costs reasonably incurred.

9                   g.       **Illinois.** Ill. Comp. Stat. Ch. 720 § 5/14-6 provides for the recovery in a civil  
 10                  action of relief for violations of Ill. Comp. Stat. Ch. 720 § 5/14-2(a)(1), which  
 11                  provides in pertinent part:

12                  § 14-2. Elements of the offense; affirmative defense.

13                  (a) A person commits eavesdropping when he:

14                   (1) Knowingly and intentionally uses an eavesdropping  
 15                   device for the purpose of hearing or recording all or any part of any  
 16                   conversation or intercepts, retains, or transcribes electronic  
 17                   communication unless he does so (A) with the consent of all of the  
 18                   parties to such conversation or electronic communication or (B) in  
 19                   accordance with Article 108A or Article 108B of the "Code of  
 20                   Criminal Procedure of 1963", approved August 14, 1963, as  
 21                   amended; or

22                  (2) Manufactures, assembles, distributes, or possesses any  
 23                  electronic, mechanical, eavesdropping, or other device knowing that  
 24                  or having reason to know that the design of the device renders it  
 25                  primarily useful for the purpose of the surreptitious hearing or  
 26                  recording of oral conversations or the interception, retention, or  
 27                  transcription of electronic communications and the intended or actual  
 28                  use of the device is contrary to the provisions of this Article; or

29                  (3) Uses or divulges, except as authorized by this Article or  
 30                  by Article 108A or 108B of the "Code of Criminal Procedure of  
 31                  1963", approved August 14, 1963, as amended, any information  
 32                  which he knows or reasonably should know was obtained through the  
 33                  use of an eavesdropping device.

34                  Defendants Carrier IQ and the Device Manufacturers, by way of their  
 35                  programming, knowing and intentional installation, activation, and other

1 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 2 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 3 authorized, employed, or procured or permitted others to so do.

4 Ill. Comp. Stat. Ch. 720 § 5/14-6 provides in pertinent part:

5       § 14-6. Civil remedies to injured parties. (1) Any or all parties  
 6 to any conversation or electronic communication upon which  
 7 eavesdropping is practiced contrary to this Article shall be entitled to  
 the following remedies:

8               (a) To an injunction by the circuit court prohibiting further  
 9 eavesdropping by the eavesdropper and by or on behalf of his  
 principal, or either;

10              (b) To all actual damages against the eavesdropper or his  
 11 principal or both;

12              (c) To any punitive damages which may be awarded by the  
 13 court or by a jury;

14              (d) To all actual damages against any landlord, owner or  
 15 building operator, or any common carrier by wire who aids, abets, or  
 knowingly permits the eavesdropping concerned;

16              (e) To any punitive damages which may be awarded by the  
 17 court or by a jury against any landlord, owner or building operator, or  
 18 common carrier by wire who aids, abets, or knowingly permits the  
 eavesdropping concerned.

19       Based on the allegations herein, plaintiffs and the class are entitled to  
 20 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 21 damages provided by the foregoing statute, including punitive damages; and a  
 22 reasonable attorney's fee and other litigation costs reasonably incurred.

23       h.       **Indiana.** Ind. Code § 35-33.5-5-4 provides for the recovery in a civil action  
 24 of relief for violations of Ind. Code § 35-33.5-2-1(1)(c), which, in pertinent part,  
 25 provides:

26               Sec. 1. (a) A prosecuting attorney or, if the prosecuting  
 27 attorney is unavailable, a chief deputy prosecuting attorney  
 28 specifically authorized by the prosecuting attorney, may submit an  
 application for a warrant or an extension to a circuit or superior court  
 where:

(1) the county that the prosecuting attorney represents is located; and

(2) the communication subject to the warrant is anticipated to be sent or received.

The prosecuting attorney or authorized chief deputy prosecuting attorney may not delegate the responsibility of applying for a warrant or an extension to another deputy prosecuting attorney.

(b) One (1) of the following persons must serve as a coapplicant for a warrant or an extension under subsection (a):

(1) The superintendent of the state police department.

(2) The police chief of a consolidated city where the communication subject to the warrant is anticipated to be sent or received.

(3) The sheriff of the county containing a consolidated city where the communication subject to the warrant is anticipated to be sent or received.

(c) Only the state police department may install equipment used to intercept an electronic communication under this chapter.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do

Ind. Code § 35-33.5-5-4 provides in pertinent part:

Sec. 4. (a) A person whose communications are intercepted, disclosed, or used in violation of this article:

(1) has a civil cause of action against a person who intercepts, discloses, uses, or procures another person to intercept, disclose, or use a communication in violation of this article; and

(2) is entitled to recover from that person the following:

(A) The greater of:

(i) actual damages;

(ii) liquidated damages computed at a rate of one hundred dollars (\$100) each day for each day of violation; or

(iii) one thousand dollars (\$1,000).

**(B) Court costs (including fees).**

(C) Punitive damages, when determined to be appropriate by the court.

(D) Reasonable attorney's fees.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

i. **Iowa.** Iowa Code § 808B.8 provides for the recovery in a civil action of relief for violations of Iowa Code § 808b.2(1)(a), (c), and (d), which, in pertinent part, provides:

1. Except as otherwise specifically provided in this chapter, a person who does any of the following commits a class "D" felony:

a. Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, a wire, oral, or electronic communication.

b. Willfully uses, endeavors to use, or procures any other person to use or endeavor to use an electronic, mechanical, or other device to intercept any oral communication when either of the following applies:

(1) The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication.

(2) The device transmits communications by radio, or interferes with the transmission of radio communications.

c. Willfully discloses, or endeavors to disclose, to any other person the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained

1 through the interception of a wire, oral, or electronic communication  
 2 in violation of this subsection.

3           d. Willfully uses, or endeavors to use, the contents of a wire,  
 4 oral, or electronic communication, knowing or having reason to  
 5 know that the information was obtained through the interception of a  
 6 wire, oral, or electronic communication in violation of this  
 7 subsection.

8           Defendants Carrier IQ and the Device Manufacturers, by way of their  
 9 programming, knowing and intentional installation, activation, and other  
 10 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 11 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 12 authorized, employed, or procured or permitted others to so do.

13           Iowa Code Ann. §808B.8 provides:

14           1. A person whose wire, oral, or electronic communication is  
 15 intercepted, disclosed, or used in violation of this chapter shall:

16           a. Have a civil cause of action against any person who  
 17 intercepts, discloses, or uses or procures any other person to  
 18 intercept, disclose, or use such communications.

19           b. Be entitled to recover from any such person all of the  
 20 following:

21           (1) Actual damages, but not less than liquidated damages  
 22 computed at the rate of one hundred dollars a day for each day of  
 23 violation, or one thousand dollars, whichever is higher.

24           (2) Punitive damages upon a finding of a willful, malicious,  
 25 or reckless violation of this chapter.

26           (3) A reasonable attorney fee and other litigation costs  
 27 reasonably incurred.

28           2. A good faith reliance on a court order shall constitute a  
 29 complete defense to any civil or criminal action brought under this  
 30 chapter.

31           3. A person whose wire, oral, or electronic communication is  
 32 intercepted, disclosed, or used in violation of this chapter may seek  
 33 an injunction, either temporary or permanent, against any person who  
 34 violates this chapter.

1                 Based on the allegations herein, plaintiffs and the class are entitled to  
 2 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 3 damages provided by the foregoing statute, including punitive damages; and a  
 4 reasonable attorney's fee and other litigation costs reasonably incurred.

5                 j.         **Louisiana.** La. Rev. Stat. § 15:1312 provides for the recovery in a civil  
 6 action of relief for violations of La. Rev. Stat. § 15:1303(A)(1), (3)-(4), which, in  
 7 pertinent part, provides:

8                         Except as otherwise specifically provided in this Chapter, it  
 9 shall be unlawful for any person to:

10                         (1) Willfully intercept, endeavor to intercept, or procure any  
 11 other person to intercept or endeavor to intercept, any wire,  
 electronic or oral communication;

12                         (2) Willfully use, endeavor to use, or procure any other  
 13 person to use or endeavor to use, any electronic, mechanical, or other  
 device to intercept any oral communication when:

14                         (a) Such device is affixed to, or otherwise transmits a signal  
 15 through, a wire, cable, or other like connection used in wire or  
 electronic communication; or

16                         (b) Such device transmits communications by radio or  
 17 interferes with the transmission of such communication;

18                         (3) Willfully disclose, or endeavor to disclose, to any other  
 19 person the contents of any wire, electronic, or oral communication,  
 20 knowing or having reason to know that the information was obtained  
 21 through the interception of a wire, electronic, or oral communication  
 in violation of this Subsection; or

22                         (4) Willfully use, or endeavor to use, the contents of any wire,  
 23 electronic, or oral communication, knowing or having reason to  
 24 know that the information was obtained through the interception of a  
 wire, electronic, or oral communication in violation of this  
 Subsection.

25                 Defendants Carrier IQ and the Device Manufacturers, by way of their  
 26 programming, knowing and intentional installation, activation, and other  
 27 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ

1           Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 2           authorized, employed, or procured or permitted others to so do.

3           La. Rev. Stat. § 15:1312 provides in pertinent part:

4           A. Any person whose wire, electronic, or oral communication  
 5           is intercepted, disclosed, or used in violation of this Chapter shall  
 6           have a civil cause of action against any person who intercepts,  
 7           discloses, or uses, or procures any other person to intercept, disclose,  
 8           or use such communications, and be entitled to recover from any  
 9           such person:

10           (1) Actual damages, but not less than liquidated damages  
 11           computed at the rate of one hundred dollars a day for each day of  
 12           violation or one thousand dollars, whichever is greater.

13           (2) A reasonable attorney's fee and other litigation costs  
 14           reasonably incurred.

15           (3) Punitive damages.

16           Based on the allegations herein, plaintiffs and the class are entitled to the  
 17           maximum damages provided by the foregoing statute, including punitive damages;  
 18           and a reasonable attorney's fee and other litigation costs reasonably incurred.

19           k.       **Maine.** Me. Rev. Stat. ch. 15 § 711 provides for the recovery in a  
 20           civil action of relief for violations of Me. Rev. Stat. ch. 15 § 710(1), which, in  
 21           pertinent part, provides:

22           1. Interception, oral communications prohibited. Any person,  
 23           other than an employee of a communication common carrier, a law  
 24           enforcement officer, an investigative officer, another employee of the  
 25           Department of Corrections authorized to exercise law enforcement  
 26           powers as described in Title 34-A, section 3011 or a jail investigative  
 27           officer or a jail employee acting at the direction of a jail investigative  
 28           officer, carrying out practices otherwise permitted by this chapter,  
 29           who intentionally or knowingly intercepts, attempts to intercept or  
 30           procures any other person to intercept or attempt to intercept any  
 31           wire or oral communication is guilty of a Class C crime.

32           2. Editing of tape recordings in judicial proceedings  
 33           prohibited. Any person who knowingly or intentionally edits, alters  
 34           or tampers with any tape, transcription or other sound recording, or  
 35           knows of such editing, altering or tampering, and presents that  
 36           recording in any judicial proceeding or proceeding under oath,

1 without fully indicating the nature of the changes made and the  
 2 original state of the recording, is guilty of a Class C crime.

3       3. Disclosure, or use of wire or oral communications  
 4 prohibited. A person is guilty of a Class C crime if he:

5           A. Intentionally or knowingly discloses or attempts to  
 6 disclose to any person the contents of any wire or oral  
 7 communication, knowing that the information was obtained through  
 8 interception; or

9           B. Intentionally or knowingly uses or attempts to use the  
 10 contents of any wire or oral communication, knowing that the  
 11 information was obtained through interception.

12       4. Duty to report. Any communications common carrier shall  
 13 promptly report to the Attorney General any facts coming to its  
 14 attention in the conduct of its business which may indicate a possible  
 15 violation of this section and such carrier shall adopt reasonable rules  
 16 to assure compliance with this subsection, provided such carrier shall  
 17 not be liable to any person who may claim an injury arising out of  
 18 any such report, if made in good faith. Any person violating this  
 19 subsection shall be subject to a civil penalty not to exceed \$5,000,  
 20 payable to the State, to be recovered in a civil action.

21       5. Possession of interception devices prohibited. A person,  
 22 other than an employee of a communication common carrier, a law  
 23 enforcement officer, an investigative officer, another employee of the  
 24 Department of Corrections authorized to exercise law enforcement  
 25 powers as described in Title 34-A, section 3011 or a jail investigative  
 26 officer or a jail employee acting at the direction of a jail investigative  
 27 officer, carrying out practices otherwise permitted by this chapter,  
 28 who has in that person's possession any device, contrivance, machine  
 or apparatus designed or commonly used for intercepting wire or oral  
 communications is guilty of a Class C crime.

29       6. Sale of interception devices prohibited. A person who sells,  
 30 exchanges, delivers, barter, gives or furnishes or possesses with an  
 31 intent to sell any device, contrivance, machine or apparatus designed  
 32 or commonly used for the interception of wire or oral  
 33 communications as defined in this chapter is guilty of a Class B  
 34 crime. This subsection shall not include devices manufactured under  
 35 written contract for sale to common carriers, law enforcement  
 36 agencies and the Department of Corrections, provided that the  
 37 production of any such device shall not have commenced prior to the  
 38 signing of the contract by both parties.

1       See also Me. Rev. Stat. ch. 15 § 709(7) (defining “wire communication” in such a  
 2 manner as to encompass electronic communications such as those here at issue).

3              Defendants Carrier IQ and the Device Manufacturers, by way of their  
 4 programming, knowing and intentional installation, activation, and other  
 5 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 6 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 7 authorized, employed, or procured or permitted others to so do.

8              Me. Rev. Stat. ch. 15 § 711 provides:

9                  Any party to a conversation intercepted, disclosed or used in  
 10 violation of this chapter shall have a civil cause of action against any  
 11 person who intercepts, discloses or uses such communications and  
 shall be entitled to recover from any such persons:

12                 1. Damages. Actual damages, but not less than liquidated  
 13 damages, computed at the rate of \$100 per day for each day of  
 violation; and

14                 2. Attorney's fee. A reasonable attorney's fee and other  
 15 litigation disbursements reasonably incurred.

16              Based on the allegations herein, plaintiffs and the class are entitled to the  
 17 maximum damages provided by the foregoing statute, including punitive damages;  
 18 and a reasonable attorney's fee and other litigation costs reasonably incurred.

19                 1.       **Maryland.** Md. Cts. & Jud. Pro. Code § 10-410 provides for the recovery in  
 20 a civil action of relief for violations of Md. Cts. & Jud. Pro. Code § 10-402, which,  
 21 in pertinent part, provides:

22                         (a) Except as otherwise specifically provided in this subtitle it  
 23 is unlawful for any person to:

24                                 (1) Willfully intercept, endeavor to intercept, or procure any  
 25 other person to intercept or endeavor to intercept, any wire, oral, or  
 electronic communication;

26                                 (2) Willfully disclose, or endeavor to disclose, to any other  
 27 person the contents of any wire, oral, or electronic communication,  
 knowing or having reason to know that the information was obtained

1           through the interception of a wire, oral, or electronic communication  
 2           in violation of this subtitle; or

3                 (3) Willfully use, or endeavor to use, the contents of any wire,  
 4                 oral, or electronic communication, knowing or having reason to  
 5                 know that the information was obtained through the interception of a  
 6                 wire, oral, or electronic communication in violation of this subtitle.

7                 *See also* Md. Cts. & Jud. Pro. Code § 10-401(5)(i) (defining “electronic  
 8                 communication”).

9                 Defendants Carrier IQ and the Device Manufacturers, by way of their  
 10                programming, knowing and intentional installation, activation, and other  
 11                involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 12                Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 13                authorized, employed, or procured or permitted others to do so.

14                 Md. Cts. & Jud. Pro. Code §10-410 provides in pertinent part:

15                 Any person whose wire, oral, or electronic communication is  
 16                 intercepted, disclosed, or used in violation of this subtitle shall have a  
 17                 civil cause of action against any person who intercepts, discloses, or  
 18                 uses, or procures any other person to intercept, disclose, or use the  
 19                 communications, and be entitled to recover from any person:

20                 (1) Actual damages but not less than liquidated damages  
 21                 computed at the rate of \$100 a day for each day of violation or  
 22                 \$1,000, whichever is higher;

23                 (2) Punitive damages; and

24                 (3) A reasonable attorney's fee and other litigation costs  
 25                 reasonably incurred.

26                 Based on the allegations herein, plaintiffs and the class are entitled to the  
 27                 maximum damages provided by the foregoing statute, including punitive damages;  
 28                 and a reasonable attorney's fee and other litigation costs reasonably incurred.

29                 m.         **Massachusetts.** Mass. Gen. Laws ch. 272 § 99(Q) provides for the  
 30                 recovery in a civil action of relief for violations of Mass. Gen. Laws ch. § 99(C)(1),  
 31                 which, in pertinent part, provides:

1                   1. Interception, oral communications prohibited.

2                   Except as otherwise specifically provided in this section any  
3                   person who—

4                   willfully commits an interception, attempts to commit an  
5                   interception, or procures any other person to commit an interception  
6                   or to attempt to commit an interception of any wire or oral  
7                   communication shall be fined not more than ten thousand dollars, or  
imprisoned in the state prison for not more than five years, or  
imprisoned in a jail or house of correction for not more than two and  
one half years, or both so fined and given one such imprisonment.

8                   Proof of the installation of any intercepting device by any  
9                   person under circumstances evincing an intent to commit an  
interception, which is not authorized or permitted by this section,  
10                  shall be *prima facie* evidence of a violation of this subparagraph.

11                  Mass. Gen. Laws ch. 272 § 99(B)(1) defines "wire communication" broadly  
12                  enough to encompass electronic communications as discussed herein.

13                  Defendants Carrier IQ and the Device Manufacturers, by way of their  
14                  programming, knowing and intentional installation, activation, and other  
15                  involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
16                  Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
17                  authorized, employed, or procured or permitted others to so do.

18                  Accordingly, plaintiffs and the class are entitled under Mass. Gen. Laws ch.  
19                  272 § 99(Q) to a civil remedy per the following:

20                  Any aggrieved person whose oral or wire communications  
21                  were intercepted, disclosed or used except as permitted or authorized  
22                  by this section or whose personal or property interests or privacy  
23                  were violated by means of an interception except as permitted or  
24                  authorized by this section shall have a civil cause of action against  
any person who so intercepts, discloses or uses such communications  
or who so violates his personal, property or privacy interest, and shall  
be entitled to recover from any such person—

25                  1. actual damages but not less than liquidated damages  
26                  computed at the rate of \$100 per day for each day of violation or  
\$1000, whichever is higher;

27                  2. punitive damages; and

1                   3. a reasonable attorney's fee and other litigation  
 2                   disbursements reasonably incurred. Good faith reliance on a warrant  
 3                   issued under this section shall constitute a complete defense to an  
 4                   action brought under this paragraph.

5                   Based on the allegations herein, plaintiffs and the class are entitled to the  
 6                   maximum damages provided by the foregoing statute, including punitive damages;  
 7                   and a reasonable attorney's fee and other litigation costs reasonably incurred.

8                   n.       **Michigan.** Mich. Stat. § 750.539h provides for the recovery in a civil action  
 9                   of relief for violations of Mich. Stat. § 750.539c, which, in pertinent part, prohibits  
 10                  “eavesdropping.” More specifically, it provides:

11                  Sec. 539c. Any person who is present or who is not present  
 12                  during a private conversation and who willfully uses any device to  
 13                  eavesdrop upon the conversation without the consent of all parties  
 14                  thereto, or who knowingly aids, employs or procures another person  
 15                  to do the same in violation of this section, is guilty of a felony  
 16                  punishable by imprisonment in a state prison for not more than 2  
 17                  years or by a fine of not more than \$2,000.00, or both.

18                  *See also* Mich. Stat. § 750.539a(2) (defining “eavesdropping” in such a manner as to  
 19                  encompass the communications here at issue, especially the recording or  
 20                  transmitting of text messages).

21                  Defendants Carrier IQ and the Device Manufacturers, by way of their  
 22                  programming, knowing and intentional installation, activation, and other  
 23                  involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 24                  Interface, have eavesdropped, and/or have aided or procured others to so do.

25                  Mich. Stat. § 750.539h provides:

26                  Sec. 539h. Any parties to any conversation upon which  
 27                  eavesdropping is practiced contrary to this act shall be entitled to the  
 28                  following civil remedies:

29                  (a) An injunction by a court of record prohibiting further  
 30                  eavesdropping.

31                  (b) All actual damages against the person who eavesdrops.

(c) Punitive damages as determined by the court or by a jury.

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

o. **Minnesota.** Minn. Stat. § 626A.13 provides for the recovery in a civil action of relief for violations of Minn. Stat. § 626A.02 (1)(1), (3)-(4), which, in pertinent part, provides:

**Subdivision 1. Offenses.** Except as otherwise specifically provided in this chapter any person who:

(1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication;

(2) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication;

(3) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; or

(4) intentionally uses, or endeavors to use, the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; shall be punished as provided in subdivision 4, or shall be subject to suit as provided in subdivision 5.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other

1 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 2 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 3 authorized, employed, or procured or permitted others to so do.

4 Minn. Stat. § 626A.13 provides in pertinent part:

5 Subdivision 1. In general. Except as provided in section  
 6 2511(2)(a)(ii) of title 18 of the United States Code, a person whose  
 7 wire, oral, or electronic communication is intercepted, disclosed, or  
 8 intentionally used in violation of this chapter may in a civil action  
 recover from the person or entity that engaged in that violation relief  
 as may be appropriate.

9 Subd. 2. Relief. In an action under this section, appropriate  
 10 relief includes:

11 (1) temporary and other equitable or declaratory relief as may  
 12 be appropriate;

13 (2) damages under subdivision 3 and punitive damages in  
 14 appropriate cases; and

15 (3) a reasonable attorney's fee and other litigation costs  
 reasonably incurred.

16 Subd. 3. Computation of damages. (a) In an action under this  
 17 section, if the conduct in violation of this chapter is the private  
 18 viewing of a private satellite video communication that is not  
 19 scrambled or encrypted or if the communication is a radio  
 20 communication that is transmitted on frequencies allocated under  
 21 subpart D of part 74 of title 47 of the Code of Federal Regulations  
 22 that is not scrambled or encrypted and the conduct is not for a  
 tortious or illegal purpose or for purposes of direct or indirect  
 23 commercial advantage or private commercial gain, then the court  
 shall assess damages as follows:

24 (1) If the person who engaged in that conduct has not  
 25 previously been enjoined under section 626A.02, subdivision 5, and  
 has not been found liable in a prior civil action under this section, the  
 court shall assess the greater of the sum of actual damages suffered  
 by the plaintiff, or statutory damages of not less than \$50 and not  
 more than \$500.

26 (2) If, on one prior occasion, the person who engaged in that  
 27 conduct has been enjoined under section 626A.02, subdivision 5, or  
 28 has been found liable in a civil action under this section, the court  
 shall assess the greater of the sum of actual damages suffered by the

1 plaintiff, or statutory damages of not less than \$100 and not more  
 2 than \$1,000.

3                         (b) In any other action under this section, the court may  
 4 assess as damages whichever is the greater of:

5                         (1) the sum of three times the actual damages suffered by the  
 6 plaintiff and any profits made by the violator as a result of the  
 7 violation; or

8                         (2) statutory damages of whichever is the greater of \$100 a  
 9 day for each day of violation or \$10,000.

10                         Based on the allegations herein, plaintiffs and the class are entitled to  
 11 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 12 damages provided by the foregoing statute, including punitive damages; and a  
 13 reasonable attorney's fee and other litigation costs reasonably incurred.

14 p.                         **Nebraska.** Neb. Rev. Stat. § 86-297 provides for the recovery in a  
 15 civil action of relief for violations of Neb. Rev. Stat. § 86-290. In pertinent part,  
 16 Neb. Rev. Stat. § 86-290 provides that

17                         it is unlawful to:

18                         (a) Intentionally intercept, endeavor to intercept, or procure  
 19 any other person to intercept or endeavor to intercept any wire,  
 20 electronic, or oral communication;

21                         (b) Intentionally use, endeavor to use, or procure any other  
 22 person to use or endeavor to use any electronic, mechanical, or other  
 23 device to intercept any oral communication when (i) such device is  
 24 affixed to, or otherwise transmits a signal through, a wire, cable, or  
 25 other like connection used in wire communication or (ii) such device  
 26 transmits communications by radio or interferes with the  
 27 transmission of such communication;

28                         (c) Intentionally disclose or endeavor to disclose to any other  
 29 person the contents of any wire, electronic, or oral communication,  
 30 knowing or having reason to know that the information was obtained  
 31 through the interception of a wire, electronic, or oral communication  
 32 in violation of this subsection;

33                         (d) Intentionally use or endeavor to use the contents of any  
 34 wire, electronic, or oral communication, knowing or having reason to

1 know that the information was obtained through the interception of a  
 2 wire, electronic, or oral communication in violation of this  
 3 subsection . . . .

4 Defendants Carrier IQ and the Device Manufacturers, by way of their  
 5 programming, knowing and intentional installation, activation, and other  
 6 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 7 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 8 authorized, employed, or procured or permitted others to so do.

9 Neb. Rev. Stat. § 86-297 provides:

10 (1) Any person whose wire, electronic, or oral  
 11 communication is intercepted, disclosed, or intentionally used in  
 12 violation of sections 86-271 to 86-295 and 86-298 to 86-2,103 may  
 13 in a civil action recover from the person or entity which engaged in  
 14 that violation such relief as may be appropriate.

15 (2) In an action under this section, appropriate relief includes:

16 (a) Such preliminary and other equitable or declaratory relief  
 17 as may be appropriate;

18 (b) Damages under subsection (3) of this section; and

19 (c) Reasonable attorney's fees and other litigation costs  
 20 reasonably incurred.

21 (3)(a) In an action under this section, if the conduct in  
 22 violation of sections 86-271 to 86-295 and 86-298 to 86-2,103 is the  
 23 private viewing of a private satellite video communication that is not  
 24 scrambled or encrypted or if the communication is a radio  
 25 communication that is transmitted on frequencies allocated for  
 26 remote pickup broadcast stations under subpart D of 47 C.F.R. part  
 27 74, as such regulations existed on January 1, 2002, that is not  
 28 scrambled or encrypted and the conduct is not for a tortious or illegal  
 purpose or for purposes of direct or indirect commercial advantage or  
 private commercial gain, then the court shall assess damages as  
 follows:

(i) If the person who engaged in such conduct has not previously been enjoined under subsection (5) of section 86-290 and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered

1 by the plaintiff or statutory damages of not less than fifty dollars and  
 2 not more than five hundred dollars; or

3                         (ii) If on one prior occasion the person who engaged in such  
 4 conduct has been enjoined under subsection (5) of section 86-290 or  
 5 has been found liable in a civil action under this section, the court  
 6 shall assess the greater of the sum of actual damages suffered by the  
 7 plaintiff or statutory damages of not less than one hundred dollars  
 8 and not more than one thousand dollars.

9                         (b) In any other action under this section, the court may  
 10 assess as damages whichever is the greater of:

11                         (i) The sum of the actual damages suffered by the plaintiff  
 12 and any profits made by the violator as a result of the violation; or

13                         (ii) Statutory damages of whichever is the greater of one  
 14 hundred dollars a day for each day of violation or ten thousand  
 15 dollars.

16                         Based on the allegations herein, plaintiffs and the class are entitled to  
 17 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 18 damages provided by the foregoing statute, including punitive damages; and a  
 19 reasonable attorney's fee and other litigation costs reasonably incurred.

20                         q.         **Nevada.** Nev. Rev. Stat. § 200.690 provides for the recovery in a  
 21 civil action of relief for violations of Nev. Rev. Stat. § 200.620, which, in pertinent  
 22 part,

23                         1. Except as otherwise provided in NRS 179.410 to 179.515,  
 24 inclusive, 209.419 and 704.195, it is unlawful for any person to  
 25 intercept or attempt to intercept any wire communication unless:

26                         (a) The interception or attempted interception is made with  
 27 the prior consent of one of the parties to the communication; and

28                         (b) An emergency situation exists and it is impractical to  
 29 obtain a court order as required by NRS 179.410 to 179.515,  
 30 inclusive, before the interception, in which event the interception is  
 31 subject to the requirements of subsection 3. If the application for  
 32 ratification is denied, any use or disclosure of the information so  
 33 intercepted is unlawful, and the person who made the interception  
 34 shall notify the sender and the receiver of the communication that:

(1) The communication was intercepted; and

(2) Upon application to the court, ratification of the interception was denied.

*See also* Nev. Rev. Stat. § 610 (2), which defines "wire communication" in such a manner as to include the electronic communications here at issue.

Nev. Rev. Stat. § 200.690 provides in pertinent part:

1. A person who willfully and knowingly violates NRS 200.620 to 200.650, inclusive;

(a) Shall be punished for a category D felony as provided in NRS 193.130.

(b) Is liable to a person whose wire or oral communication is intercepted without his or her consent for:

(1) Actual damages or liquidated damages of \$100 per day of violation but not less than \$1,000, whichever is greater:

## (2) Punitive damages; and

(3) His or her costs reasonably incurred in the action, including a reasonable attorney's fee.

all of which may be recovered by civil action.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

r.       **New Hampshire.** N.H. Rev. Stat. § 570-A:11 provides for the recovery in a civil action of relief for violations of N.H. Rev. Stat. § 570-A:2, which, in pertinent part, provides:

I. A person is guilty of a class B felony if, except as otherwise specifically provided in this chapter or without the consent of all parties to the communication, the person:

(a) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any telecommunication or oral communication:

(b) Wilfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(1) Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in telecommunication, or

(2) Such device transmits communications by radio, or interferes with the transmission of such communication, or

(3) Such use or endeavor to use (A) takes place on premises of any business or other commercial establishment, or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment; or

(c) Wilfully discloses, or endeavors to disclose, to any other person the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of this paragraph; or

(d) Willfully uses, or endeavors to use, the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of this paragraph.

*See also* N.H. Rev. Stat. § 570-A:1 (I), which defines “telecommunication” in such a manner as to include the electronic communications here at issue.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

N.H. Rev. Stat. § 570-A:11 provides:

Any person whose telecommunication or oral communication is intercepted, disclosed, or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose or use such communications, and be entitled to recover from any

1                   such person: (a) actual damages but not less than liquidated damages  
 2                   computed at the rate of \$100 a day for each day of violation or  
 3                   \$1,000, whichever is higher; (b) punitive damages; and (c) a  
 4                   reasonable attorney's fee and other litigation costs reasonably  
 5                   incurred. Good faith reliance on a court order or on a representation  
 6                   made by the attorney general, deputy attorney general or a county  
 7                   attorney shall constitute a complete defense to any civil or criminal  
 8                   action brought under this chapter.

9                   Based on the allegations herein, plaintiffs and the class are entitled to the  
 10                  maximum damages provided by the foregoing statute, including punitive damages;  
 11                  and a reasonable attorney's fee and other litigation costs reasonably incurred.

12                 s.        **New Jersey.** N.J. Stat. Ann. § 2A:156A-24 provides for the recovery  
 13                  in a civil action of relief for violations of N.J. Stat. § 2A:156A-3, which, in pertinent  
 14                  part, provides:

15                   Except as otherwise specifically provided in this act, any  
 16                   person who:

17                   a. Purposely intercepts, endeavors to intercept, or procures  
 18                   any other person to intercept or endeavor to intercept any wire,  
 19                   electronic or oral communication; or

20                   b. Purposely discloses or endeavors to disclose to any other  
 21                   person the contents of any wire, electronic or oral communication, or  
 22                   evidence derived therefrom, knowing or having reason to know that  
 23                   the information was obtained through the interception of a wire,  
 24                   electronic or oral communication; or

25                   c. Purposely uses or endeavors to use the contents of any  
 26                   wire, electronic or oral communication, or evidence derived  
 27                   therefrom, knowing or having reason to know, that the information  
 28                   was obtained through the interception of a wire, electronic or oral  
 29                   communication;

30                   shall be guilty of a crime of the third degree. Subsections b.  
 31                   and c. of this section shall not apply to the contents of any wire,  
 32                   electronic or oral communication, or evidence derived therefrom, that  
 33                   has become common knowledge or public information.

34                   Defendants Carrier IQ and the Device Manufacturers, by way of their  
 35                   programming, knowing and intentional installation, activation, and other  
 36                   involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ

1           Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 2           authorized, employed, or procured or permitted others to so do.

3           N.J. Stat. § 2A:156A-24 provides:

4           Any person whose wire, electronic or oral communication is  
 5           intercepted, disclosed or used in violation of this act shall have a civil  
 6           cause of action against any person who intercepts, discloses or uses  
 7           or procures any other person to intercept, disclose or use, such  
 8           communication; and shall be entitled to recover from any such  
 9           person:

10           a. Actual damages, but not less than liquidated damages  
 11           computed at the rate of \$100.00 a day for each day of violation, or  
 12           \$1,000.00, whichever is higher;

13           b. Punitive damages; and

14           c. A reasonable attorney's fee and other litigation costs  
 15           reasonably incurred.

16           Based on the allegations herein, plaintiffs and the class are entitled to the  
 17           maximum damages provided by the foregoing statute, including punitive damages;  
 18           and a reasonable attorney's fee and other litigation costs reasonably incurred.

19           t.       **New Mexico.** N.M. Stat. § 30-12-11 provides for the recovery in a  
 20           civil action of relief for violations of N.M. Stat. § 30-12-1, which, in pertinent part,  
 21           provides:

22           Interference with communications consists of knowingly and  
 23           without lawful authority:

24           A. displacing, removing, injuring or destroying any radio  
 25           station, television tower, antenna or cable, telegraph or telephone  
 26           line, wire, cable, pole or conduit belonging to another, or the material  
 27           or property appurtenant thereto;

28           B. cutting, breaking, tapping or making any connection with  
 29           any telegraph or telephone line, wire, cable or instrument belonging  
 30           to or in the lawful possession or control of another, without the  
 31           consent of such person owning, possessing or controlling such  
 32           property;

33           C. reading, interrupting, taking or copying any message,  
 34           communication or report intended for another by telegraph or

1                   telephone without the consent of a sender or intended recipient  
2                   thereof;

3                   D. preventing, obstructing or delaying the sending,  
4                   transmitting, conveying or delivering in this state of any message,  
5                   communication or report by or through telegraph or telephone; or

6                   E. using any apparatus to do or cause to be done any of the  
7                   acts hereinbefore mentioned or to aid, agree with, comply or conspire  
8                   with any person to do or permit or cause to be done any of the acts  
9                   hereinbefore mentioned.

10                  Defendants Carrier IQ and the Device Manufacturers, by way of their  
11                  programming, knowing and intentional installation, activation, and other  
12                  involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
13                  Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
14                  authorized, employed, or procured or permitted others to so do.

15                  N.M. Stat. § 30-12-11 provides in pertinent part:

16                  A. Any person whose wire or oral communication is  
17                  intercepted, disclosed or used in violation of this act shall:

18                  (1) have a civil cause of action against any person who  
19                  intercepts, discloses or uses, or procures any other person to  
20                  intercept, disclose or use such communications; and

21                  (2) be entitled to recover from any such person actual  
22                  damages, but not less than liquidated damages computed at the rate  
23                  of one hundred dollars (\$100) for each day of violation or one  
24                  thousand dollars (\$1,000), whichever is higher; punitive damages;  
25                  and a reasonable attorney's fee and other litigation costs reasonably  
26                  incurred.

27                  Based on the allegations herein, plaintiffs and the class are entitled to the  
28                  maximum damages provided by the foregoing statute, including punitive damages;  
29                  and a reasonable attorney's fee and other litigation costs reasonably incurred.

30                  u.         **North Carolina.** N.C. Gen. Stat. § 15A-296 provides for the recovery in a  
31                  civil action of relief for violations of N.C. Gen. Stat. § 15A-287, which, in pertinent  
32                  part, provides:

(a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if, without the consent of at least one party to the communication, the person:

(1) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.

(2) Willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

a. The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communications; or

b. The device transmits communications by radio, or interferes with the transmission of such communications.

(3) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through violation of this Article; or

(4) Willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Article.

*See also* N.C. Gen. Stat. § 15A-226(8) (defining “electronic communication”).

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

N.C. Gen. Stat. § 15A-296 provides:

(a) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this Article, has a civil cause of action against any person who intercepts, discloses, uses, or procures any other person to intercept, disclose, or use such communications, and is entitled to recover from any other person:

(1) Actual damages, but not less than liquidated damages, computed at the rate of one hundred dollars (\$100.00) a day for each day of violation or one thousand dollars (\$1,000), whichever is higher;

(2) Punitive damages; and

(3) A reasonable attorneys' fee and other litigation costs reasonably incurred.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

v.      **Ohio.** Ohio Rev. Code § 2933.65 provides for the recovery in a civil action of relief for violations of Ohio Rev. Code § 2933.52, which, in pertinent part, provides:

(A) No person purposely shall do any of the following:

(1) Intercept, attempt to intercept, or procure another person to intercept or attempt to intercept a wire, oral, or electronic communication;

(2) Use, attempt to use, or procure another person to use or attempt to use an interception device to intercept a wire, oral, or electronic communication, if either of the following applies:

(a) The interception device is affixed to, or otherwise transmits a signal through, a wire, cable, satellite, microwave, or other similar method of connection used in wire communications;

(b) The interception device transmits communications by radio, or interferes with the transmission of communications by radio.

(3) Use, or attempt to use, the contents of a wire, oral, or electronic communication, knowing or having reason to know that the contents were obtained through the interception of a wire, oral, or electronic communication in violation of sections 2933.51 to 2933.66 of the Revised Code.

*See also* Ohio Rev. Code § 2933.51(N) (defining “electronic communication”).

1                   Defendants Carrier IQ and the Device Manufacturers, by way  
 2 of their programming, knowing and intentional installation,  
 3 activation, and other involvement with the Carrier IQ Software,  
 4 consisting of the IQ Agent and CIQ Interface, have intentionally  
 5 intercepted, endeavored to intercept, and/or have aided, authorized,  
 6 employed, or procured or permitted others to do so.  
 7                   Ohio Rev. Code § 2933.65 provides:

8                   (A) A person whose wire, oral, or electronic communications  
 9 are intercepted, disclosed, or intentionally used in violation  
 10 of sections 2933.51 to 2933.66 of the Revised Code may bring a civil  
 11 action to recover from the person or entity that engaged in the  
 12 violation any relief that may be appropriate and that includes, but is  
 13 not limited to, the following:

14                   (1) The preliminary and other equitable or declaratory relief  
 15 that is appropriate;

16                   (2) Whichever of the following is greater:

17                   (a) Liquidated damages computed at a rate of two hundred  
 18 dollars per day for each day of violation or liquidated damages of ten  
 19 thousand dollars, whichever is greater;

20                   (b) The sum of actual damages suffered by the plaintiff and  
 21 the profits, if any, made as a result of the violation by the person or  
 22 entity that engaged in the violation.

23                   (3) Punitive damages, if appropriate;

24                   (4) Reasonable attorney's fees and other litigation expenses  
 25 that are reasonably incurred in bringing the civil action.

26                   Based on the allegations herein, plaintiffs and the class are entitled to  
 27 preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 28 damages provided by the foregoing statute, including punitive damages; and a  
 reasonable attorney's fee and other litigation costs reasonably incurred.

29                   w.       **Oregon.** Ore. Rev. Stat. §133.739 provides for the recovery in a civil action  
 30 of relief for violations of Ore. Rev. Stat. § 165.543, which provides:

31                   (1) Except as provided in ORS 133.724 or as provided  
 32 in ORS 165.540 (2)(a), any person who willfully intercepts, attempts  
 33 to intercept or procures any other person to intercept or attempt to  
 34 intercept any wire or oral communication where such person is not a  
 35 party to the communication and where none of the parties to the

1 communication has given prior consent to the interception, is guilty  
 2 of a Class A misdemeanor.

3                         (2) As used in this section, the terms “intercept” and “wire or  
 4 oral communication” have the meanings provided under ORS  
 5 133.721.

6 Defendants Carrier IQ and the Device Manufacturers, by way of their  
 7 programming, knowing and intentional installation, activation, and other  
 8 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 9 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 10 authorized, employed, or procured or permitted others to so do.

11                         Ore. Rev. Stat. §133.739 provides:

12                         (1) Any person whose wire, electronic or oral communication  
 13 was intercepted, disclosed or used in violation of ORS 133.724 or  
 14 133.737 shall have a civil cause of action against any person who  
 15 willfully intercepts, discloses or uses, or procures any other person to  
 16 intercept, disclose or use such communication and shall be entitled to  
 17 recover from any such person:

18                         (a) Actual damages but not less than damages computed at  
 19 the rate of \$100 a day for each day of violation or \$1,000, whichever  
 20 is greater; and

21                         (b) Punitive damages.

22                         (2) A good faith reliance on a court order or legislative  
 23 authorization shall constitute a complete defense to any civil action  
 24 brought under this section.

25                         (3) Nothing in ORS 41.910, 133.721 to 133.739  
 26 and 133.992 is intended to abrogate any other private civil remedy  
 27 for invasion of privacy.

28                         (4) Except as provided in subsection (5) of this section, the  
 29 court may award reasonable attorney fees to the prevailing party in  
 30 an action under this section.

31                         (5) The court may not award attorney fees to a prevailing  
 32 defendant under the provisions of subsection (4) of this section if the  
 33 action under this section is maintained as a class action pursuant  
 34 to ORCP 32.

1           Based on the allegations herein, plaintiffs and the class are entitled to the  
 2 maximum damages provided by the foregoing statute, including punitive damages;  
 3 and a reasonable attorney's fee and other litigation costs reasonably incurred.

4       x.     **Pennsylvania.** 18 Pa. Consol. Stat. § 5725 provides for the recovery in a  
 5 civil action of relief for violations of 18 Pa. Consol. Stat. § , which, in pertinent part,  
 6 provides:

7                   Except as otherwise provided in this chapter, a person is  
 8 guilty of a felony of the third degree if he:

9                   (1) intentionally intercepts, endeavors to intercept, or  
 10 procures any other person to intercept or endeavor to intercept any  
 wire, electronic or oral communication;

11                  (2) intentionally discloses or endeavors to disclose to any  
 12 other person the contents of any wire, electronic or oral  
 communication, or evidence derived therefrom, knowing or having  
 13 reason to know that the information was obtained through the  
 interception of a wire, electronic or oral communication; or

14                  (3) intentionally uses or endeavors to use the contents of any  
 15 wire, electronic or oral communication, or evidence derived  
 16 therefrom, knowing or having reason to know, that the information  
 17 was obtained through the interception of a wire, electronic or oral  
 communication.

18               *See also* 18 Pa. Consol. Stat. § 5702 (defining "electronic communication").

19               Defendants Carrier IQ and the Device Manufacturers, by way of their  
 20 programming, knowing and intentional installation, activation, and other  
 21 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 22 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 23 authorized, employed, or procured or permitted others to so do.

24               18 Pa. Consol. Stat. § 5725 provides in pertinent part:

25                  a) Cause of action.--Any person whose wire, electronic or  
 26 oral communication is intercepted, disclosed or used in violation of  
 27 this chapter shall have a civil cause of action against any person who  
 28 intercepts, discloses or uses or procures any other person to intercept,  
 disclose or use, such communication; and shall be entitled to recover  
 from any such person:

1                             (1) Actual damages, but not less than liquidated damages  
 2                             computed at the rate of \$100 a day for each day of violation, or  
 3                             \$1,000, whichever is higher.

4                             (2) Punitive damages.

5                             (3) A reasonable attorney's fee and other litigation costs  
 6                             reasonably incurred.

7                             Based on the allegations herein, plaintiffs and the class are entitled to the  
 8                             maximum damages provided by the foregoing statute, including punitive damages;  
 9                             and a reasonable attorney's fee and other litigation costs reasonably incurred.

10                         y.         **Rhode Island.** R.I. Gen. Laws. § 12-5.1-13 provides for the recovery in a  
 11                         civil action of relief for violations of R.I. Gen. Laws. § 11-35-21, which, in pertinent  
 12                         part, provides:

13                             (a) Except as otherwise specifically provided in chapter 5.1 of  
 14                             title 12, any person: (1) who willfully intercepts, attempts to  
 15                             intercept, or procures any other person to intercept or attempt to  
 16                             intercept, any wire, electronic, or oral communication; (2) who  
 17                             willfully discloses or attempts to disclose to any person the contents  
 18                             of any wire, electronic, or oral communication, knowing, or having  
 19                             reason to know that the information was obtained through  
 20                             interception of a wire, electronic, or oral communication in violation  
 21                             of this section; or (3) who willfully uses or attempts to use the  
 22                             contents of any wire, electronic, or oral communication, knowing, or  
 23                             having reason to know, that the information was obtained through  
 24                             interception of a wire, electronic, or oral communication in violation  
 25                             of this section; shall be imprisoned for not more than five (5) years.

26                             Defendants Carrier IQ and the Device Manufacturers, by way of their  
 27                             programming, knowing and intentional installation, activation, and other  
 28                             involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 authorized, employed, or procured or permitted others to so do.

26                             R.I. Gen. Laws. § 12-5.1-13 provides:

27                             (a) Any person whose wire, electronic, or oral communication  
 28                             is intercepted, disclosed, or used in violation of this chapter shall  
 have a civil cause of action against any person who intercepts,

1 discloses, or uses the communications, and shall be entitled to  
 2 recover from that person:

3                   (1) Actual damages, but not less than liquidated damages,  
 4 computed at the rate of one hundred dollars (\$100) per day for each  
 5 day of violation, or one thousand dollars (\$1,000), whichever is  
 6 higher;

7                   (2) Punitive damages; and

8                   (3) Reasonable attorneys' fees and other litigation  
 9 disbursements reasonably incurred.

10                  Based on the allegations herein, plaintiffs and the class are entitled to the  
 11 maximum damages provided by the foregoing statute, including punitive damages;  
 12 and a reasonable attorney's fee and other litigation costs reasonably incurred.

13 z.               **South Carolina.** S.C. Code Laws § 17-30-135 provides for the recovery in a  
 14 civil action of relief for violations of S.C. Code Laws § 17-30-20, which, in  
 15 pertinent part, provides:

16                  Except as otherwise specifically provided in this chapter, a  
 17 person who commits any of the following acts is guilty of a felony  
 18 and, upon conviction, must be punished as provided in Section 17-  
 19 30-50 of this chapter:

20                  (1) intentionally intercepts, attempts to intercept, or procures  
 21 any other person to intercept or attempt to intercept any wire, oral, or  
 22 electronic communication;

23                  (2) intentionally uses, attempts to use, or procures any other  
 24 person to use or attempt to use any electronic, mechanical, or other  
 25 device to intercept any oral communication when:

26                   (a) the device is affixed to or otherwise transmits a signal  
 27 through a wire, cable, or other like connection used in wire  
 28 communication; or

29                  (b) the device transmits communications by radio or  
 30 interferes with the transmission of the communication;

31                  (3) intentionally discloses or attempts to disclose to any other  
 32 person the contents of any wire, oral, or electronic communication,  
 33 knowing or having reason to know that the information was obtained

1 through the interception of a wire, oral, or electronic communication  
 2 in violation of this subsection;

3                         (4) intentionally uses or attempts to use the contents of any  
 4 wire, oral, or electronic communication, knowing or having reason to  
 5 know that the information was obtained through the interception of a  
 6 wire, oral, or electronic communication in violation of this  
 7 subsection;

8                         (5) intentionally discloses or attempts to disclose to any other  
 9 person the contents of any wire, oral, or electronic communication  
 10 intercepted by means authorized by Section 17-30-70 or Section 17-  
 11 30-95 when that person knows or has reason to know that the  
 12 information was obtained through the interception of such a  
 13 communication in connection with a criminal investigation and the  
 14 disclosure is not otherwise authorized under this chapter . . . .

15                         *See also S.C. Code Laws § 17-30-15(13) (defining “electronic communication”).*

16                         Defendants Carrier IQ and the Device Manufacturers, by way of their  
 17 programming, knowing and intentional installation, activation, and other  
 18 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 19 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 20 authorized, employed, or procured or permitted others to so do.

21                         S.C. Code Laws § 17-30-135 provides in pertinent part:

22                         (A) Any person whose wire, oral, or electronic  
 23 communication is intercepted, disclosed, or used in violation of this  
 24 chapter has a civil cause of action against any person or entity who  
 25 intercepts, discloses, or uses, or procures any other person or entity to  
 26 intercept, disclose, or use the communications and is entitled to  
 27 recover from the person or entity which engaged in that violation  
 28 relief as may be appropriate, including:

29                         (1) preliminary or equitable or declaratory relief as may be  
 30 appropriate;

31                         (2) actual damages, but not less than liquidated damages  
 32 computed at the rate of five hundred dollars a day for each day of  
 33 violation or twenty-five thousand dollars, whichever is greater, not to  
 34 exceed the limits on liability provided in subsection (F)(3);

35                         (3) punitive damages, except as may be prohibited in  
 36 subsection (F)(4); and

(4) a reasonable attorney's fee and other litigation costs reasonably incurred.

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

aa. **Tennessee.** Tenn. Code Ann. §39-13-603 provides for the recovery in a civil action of relief for violations of Tenn. Code Ann. § , which, in pertinent part, provides:

(a)(1) Except as otherwise specifically provided in §§ 39-13-601--39-13-603 and title 40, chapter 6, part 3, a person commits an offense who:

(A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(B) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(i) The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) The device transmits communications by radio, or interferes with the transmission of the communication;

(C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (a); or

(D) Intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know, that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection (a).

(2) A violation of subdivision (a)(1) shall be punished as provided in § 39-13-602 and shall be subject to suit as provided in § 39-13-603.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Tenn. Code Ann. § 39-13-603 provides:

a) Except as provided in § 39-13-601(b)(4), any aggrieved person whose wire, oral or electronic communication is intentionally intercepted, disclosed, or used in violation of § 39-13-601 or title 40, chapter 6, part 3 may in a civil action recover from the person or entity that engaged in that violation the following relief:

(1) The greater of:

(A) The sum of the actual damages, including any damage to personal or business reputation or relationships, suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) Statutory damages of one hundred dollars (\$100) a day for each day of violation or ten thousand dollars (\$10,000), whichever is greater;

(2) Punitive damages; and

(3) A reasonable attorney's fee and other litigation costs reasonably incurred.

(b) Any person whose wire, oral, or electronic communication is or is about to be intercepted, disclosed, or used in violation of § 39-13-601 or title 40, chapter 6, part 3 may seek to enjoin and restrain the violation and may in the same action seek damages as provided by subsection (a).

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum

1 damages provided by the foregoing statute, including punitive damages; and a  
 2 reasonable attorney's fee and other litigation costs reasonably incurred.

3 bb. **Texas.** Tex. Code Crim. Pro. Art. 18.20 provides for the recovery in a civil  
 4 action of relief for violations of Tex. Penal Code § 16.02 , which, in pertinent part,  
 5 provides:

6                 (a) In this section, "computer trespasser," "covert entry,"  
 7 "communication common carrier," "contents," "electronic  
 8 communication," "electronic, mechanical, or other device,"  
 9 "immediate life-threatening situation," "intercept," "investigative or  
 10 law enforcement officer," "member of a law enforcement unit  
 11 specially trained to respond to and deal with life-threatening  
 situations," "oral communication," "protected computer," "readily  
 accessible to the general public," and "wire communication" have the  
 meanings given those terms in Article 18.20, Code of Criminal  
 Procedure.

12                 (b) A person commits an offense if the person:

13                         (1) intentionally intercepts, endeavors to intercept, or  
 14 procures another person to intercept or endeavor to intercept a wire,  
 15 oral, or electronic communication;

16                         (2) intentionally discloses or endeavors to disclose to another  
 17 person the contents of a wire, oral, or electronic communication if  
 18 the person knows or has reason to know the information was  
 obtained through the interception of a wire, oral, or electronic  
 communication in violation of this subsection;

19                         (3) intentionally uses or endeavors to use the contents of a  
 20 wire, oral, or electronic communication if the person knows or is  
 21 reckless about whether the information was obtained through the  
 22 interception of a wire, oral, or electronic communication in violation  
 of this subsection;

23                         (4) knowingly or intentionally effects a covert entry for the  
 24 purpose of intercepting wire, oral, or electronic communications  
 without court order or authorization; or

25                         (5) intentionally uses, endeavors to use, or procures any other  
 26 person to use or endeavor to use any electronic, mechanical, or other  
 27 device to intercept any oral communication when the device:

28                                 (A) is affixed to, or otherwise transmits a signal through a  
 wire, cable, or other connection used in wire communications; or

(B) transmits communications by radio or interferes with the transmission of communications by radio.

*See also* Tex. Code Crim. Pro. Art. Sec. 18.20(15) (defining “electronic communication”).

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Tex. Code Crim. Pro. Art. 18.20 provides in pertinent part:

Sec. 16. (a) A person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this article, or in violation of Chapter 16, Penal Code, has a civil cause of action against any person who intercepts, discloses, or uses or solicits another person to intercept, disclose, or use the communication and is entitled to recover from the person:

(1) actual damages but not less than liquidated damages computed at a rate of \$100 a day for each day of violation or \$1,000, whichever is higher;

(2) punitive damages; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

cc.     **Utah.** Utah Code §§ 77-23a-11 and 77-23b-8 provide for the recovery in a civil action of relief for violations of Utah Code § 77-23a-4, which, in pertinent part, provides:

(1)(a) Except as otherwise specifically provided in this chapter, any person who violates Subsection (1)(b) is guilty of an

1 offense and is subject to punishment under Subsection (10), or when  
 2 applicable, the person is subject to civil action under Subsection (11).

3                   (b) A person commits a violation of this subsection who:

4                   (i) intentionally or knowingly intercepts, endeavors to  
 5 intercept, or procures any other person to intercept or endeavor to  
 intercept any wire, electronic, or oral communication;

6                   (ii) intentionally or knowingly uses, endeavors to use, or  
 7 procures any other person to use or endeavor to use any electronic,  
 8 mechanical, or other device to intercept any oral communication,  
 9 when the device is affixed to, or otherwise transmits a signal through  
 10 a wire, cable, or other like connection used in wire communication or  
 11 when the device transmits communications by radio, or interferes  
 12 with the transmission of the communication;

13                   (iii) intentionally or knowingly discloses or endeavors to  
 14 disclose to any other person the contents of any wire, electronic, or  
 15 oral communication, knowing or having reason to know that the  
 16 information was obtained through the interception of a wire,  
 17 electronic, or oral communication in violation of this section; or

18                   (iv) intentionally or knowingly uses or endeavors to use the  
 19 contents of any wire, electronic, or oral communication, knowing or  
 20 having reason to know that the information was obtained through the  
 21 interception of a wire, electronic, or oral communication in violation  
 22 of this section.

23                 *See also Utah Code § 77-23a-3(5) (defining “electronic communication”).*

24                 Defendants Carrier IQ and the Device Manufacturers, by way of their  
 25 programming, knowing and intentional installation, activation, and other  
 26 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 27 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 28 authorized, employed, or procured or permitted others to so do.

Utah Code § 77-23a-11 provides:

(1) Except under Subsections 77-23a-4 (3), (4), and (5), a person whose wire, electronic, or oral communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover relief as appropriate from the person or entity that engaged in the violation.

(2) In an action under this section appropriate relief includes:

(a) preliminary and other equitable or declaratory relief as is appropriate;

(b) damages under Subsection (3) and punitive damages in appropriate cases; and

(c) a reasonable attorney's fee and reasonably incurred litigation costs.

(3)(a) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted, or if the communication is a radio communication that is transmitted on frequencies allocated under Subpart (D), Part 74, Rules of the Federal Communications Commission, that is not scrambled or encrypted, and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, the court shall assess damages as follows:

(i) if the person who engaged in the conduct has not previously been enjoined under Subsection 77-23a-4 (11) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or the statutory damages of not less than \$50 nor more than \$500;

(ii) if on one prior occasion the person who engaged in the conduct has been enjoined under Subsection 77-23a-4 (11) or has been liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1,000;

(b) in any other action under this section, the court may assess as damages whichever is the greater of:

(i) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violations; or

(ii) statutory damages of \$100 a day for each day of violation, or \$10,000, whichever is greater.

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum

1 damages provided by the foregoing statute, including punitive damages; and a  
 2 reasonable attorney's fee and other litigation costs reasonably incurred.

3 dd. **Virginia.** Va. Code § 19.2-69 provides for the recovery in a civil action of  
 4 relief for violations of Va. Code § 19.2-62, which, in pertinent part, provides:

5       A. Except as otherwise specifically provided in this chapter  
 6       any person who:

7           1. Intentionally intercepts, endeavors to intercept or procures  
 8           any other person to intercept or endeavor to intercept, any wire,  
 9           electronic or oral communication;

10          2. Intentionally uses, endeavors to use, or procures any other  
 11          person to use or endeavor to use any electronic, mechanical or other  
 12          device to intercept any oral communication;

13          3. Intentionally discloses, or endeavors to disclose, to any  
 14          other person the contents of any wire, electronic or oral  
 15          communication knowing or having reason to know that the  
 16          information was obtained through the interception of a wire,  
 17          electronic or oral communication; or

18          4. Intentionally uses, or endeavors to use, the contents of any  
 19          wire, electronic or oral communication, knowing or having reason to  
 20          know that the information was obtained through the interception of a  
 21          wire, electronic or oral communication; shall be guilty of a Class 6  
 22          felony.

23       *See also* Va. Code § 19.2-61 (defining "electronic communication").

24       Defendants Carrier IQ and the Device Manufacturers, by way of their  
 25       programming, knowing and intentional installation, activation, and other  
 26       involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 27       Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 28       authorized, employed, or procured or permitted others to so do.

29       Va. Code § 19.2-69 provides in pertinent part:

30           Any person whose wire, electronic or oral communication is  
 31           intercepted, disclosed or used in violation of this chapter shall (i)  
 32           have a civil cause of action against any person who intercepts,  
 33           discloses or uses, or procures any other person to intercept, disclose  
 34           or use such communications, and (ii) be entitled to recover from any  
 35           such person:

1                   1. Actual damages but not less than liquidated damages  
 2                   computed at the rate of \$400 a day for each day of violation or  
 3                   \$4,000, whichever is higher;

4                   2. Punitive damages; and

5                   3. A reasonable attorney's fee and other litigation costs  
 6                   reasonably incurred.

7                   Based on the allegations herein, plaintiffs and the class are entitled to  
 8                   preliminary or equitable or declaratory relief as may be appropriate; the maximum  
 9                   damages provided by the foregoing statute, including punitive damages; and a  
 10                  reasonable attorney's fee and other litigation costs reasonably incurred.

11                 ee.      **Washington.** Wash. Rev. Code § 9.73.060 provides for the recovery  
 12                 in a civil action of relief for violations of Wash. Rev. Code § 9.73.030, which, in  
 13                 pertinent part, provides:

14                 1) Except as otherwise provided in this chapter, it shall be  
 15                 unlawful for any individual, partnership, corporation, association, or  
 16                 the state of Washington, its agencies, and political subdivisions to  
 17                 intercept, or record any:

18                 (a) Private communication transmitted by telephone,  
 19                 telegraph, radio, or other device between two or more individuals  
 20                 between points within or without the state by any device electronic or  
 21                 otherwise designed to record and/or transmit said communication  
 22                 regardless how such device is powered or actuated, without first  
 23                 obtaining the consent of all the participants in the communication;

24                 (b) Private conversation, by any device electronic or  
 25                 otherwise designed to record or transmit such conversation regardless  
 26                 how the device is powered or actuated without first obtaining the  
 27                 consent of all the persons engaged in the conversation.

28                 (2) Notwithstanding subsection (1) of this section, wire  
 29                 communications or conversations (a) of an emergency nature, such as  
 30                 the reporting of a fire, medical emergency, crime, or disaster, or (b)  
 31                 which convey threats of extortion, blackmail, bodily harm, or other  
 32                 unlawful requests or demands, or (c) which occur anonymously or  
 33                 repeatedly or at an extremely inconvenient hour, or (d) which relate  
 34                 to communications by a hostage holder or barricaded person as

defined in RCW 70.85.100, whether or not conversation ensues, may be recorded with the consent of one party to the conversation.

(3) Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded.

(4) An employee of any regularly published newspaper, magazine, wire service, radio station, or television station acting in the course of bona fide news gathering duties on a full-time or contractual or part-time basis, shall be deemed to have consent to record and divulge communications or conversations otherwise prohibited by this chapter if the consent is expressly given or if the recording or transmitting device is readily apparent or obvious to the speakers. Withdrawal of the consent after the communication has been made shall not prohibit any such employee of a newspaper, magazine, wire service, or radio or television station from divulging the communication or conversation.

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Wash. Rev. Code §9.73.060 provides:

Any person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute and a reasonable attorney's fee and other litigation costs reasonably incurred.

ff.      **West Virginia.** W. Va. Code § 62-1D-12 provides for the recovery in a civil action of relief for violations of W. Va. Code § 62-1D-3, which, in pertinent part, provides:

a) Except as otherwise specifically provided in this article it is unlawful for any person to:

(1) Intentionally intercept, attempt to intercept or procure any other person to intercept or attempt to intercept, any wire, oral or electronic communication; or

(2) Intentionally disclose or intentionally attempt to disclose to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this article; and

(3) Intentionally use or disclose or intentionally attempt to use or disclose the contents of any wire, oral or electronic communication or the identity of any party thereto, knowing or having reason to know that such information was obtained through the interception of a wire, oral or electronic communication in violation of this article.

(b) Any person who violates subsection (a) of this section is guilty of a felony and, upon conviction thereof, shall be imprisoned in the penitentiary for not more than five years or fined not more than ten thousand dollars or both fined and imprisoned.

*See also* W. Va. Code § 62-1D-3(n) (defining “electronic communication”).

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

W. Va. Code § 62-1D-12 provides in pertinent part:

(a) Any person whose wire, oral or electronic communication is intercepted, disclosed, used or whose identity is disclosed in violation of this article shall have a civil cause of action against any person who so intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use the communications, and shall be entitled to recover from any such person or persons:

(1) Actual damages, but not less than one hundred dollars for each day of violation;

(2) Punitive damages, if found to be proper; and

(3) Reasonable attorney fees and reasonable costs of litigation incurred.

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

gg.      **Wisconsin.** Wis. Stat. Ann. § 968.31 provides for the recovery in a civil action of relief for violations of Wis. Stat. Ann. § 968.31, which, in pertinent part, provides:

Except as otherwise specifically provided in ss. 196.63 or 968.28 to 968.30, whoever commits any of the acts enumerated in this section is guilty of a Class H felony:

(a) Intentionally intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire, electronic or oral communication.

(b) Intentionally uses, attempts to use or procures any other person to use or attempt to use any electronic, mechanical or other device to intercept any oral communication.

(c) Discloses, or attempts to disclose, to any other person the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section.

(d) Uses, or attempts to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section.

(e) Intentionally discloses the contents of any oral, electronic or wire communication obtained by authority of ss. 968.28, 968.29 and 968.30, except as therein provided. . . .

*See also* Wisc. Stat. § 968.27(4) (defining “electronic communication”).

Defendants Carrier IQ and the Device Manufacturers, by way of their programming, knowing and intentional installation, activation, and other involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ Interface, have intentionally intercepted, endeavored to intercept, and/or have aided, authorized, employed, or procured or permitted others to so do.

Wis. Stat. Ann. § 968.31 also provides in pertinent part:

2m) Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of ss. 968.28 to 968.37 shall have a civil cause of action against any person who intercepts, discloses or uses, or procures any other person to intercept, disclose, or use, the communication, and shall be entitled to recover from any such person:

(a) Actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher:

(b) Punitive damages; and

(c) A reasonable attorney's fee and other litigation costs reasonably incurred.

Based on the allegations herein, plaintiffs and the class are entitled to preliminary or equitable or declaratory relief as may be appropriate; the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

hh. **Wyoming.** Wyo. Stat. § 7-3-710 provides for the recovery in a civil action of relief for violations of Wyo. Stat. § 7-3-702, which, in pertinent part, provides:

- 1                   a) Except as provided in subsection (b) of this section, no  
 2 person shall intentionally:  
 3                   (i) Intercept, attempt to intercept, or procure any other person  
 4 to intercept or attempt to intercept any wire, oral or electronic  
 5 communication;  
 6                   (ii) Use, attempt to use, or procure any other person to use or  
 7 attempt to use any electronic, mechanical or other device to intercept  
 8 any oral communication when:  
 9                   (A) Such device is affixed to, or otherwise transmits a signal  
 10 through, a wire, cable or other like connection used in wire  
 11 communication; or  
 12                   (B) Such device transmits communications by radio or  
 13 interferes with the transmission of such communication.  
 14                   (iii) Disclose or attempt to disclose to another person the  
 15 contents of any wire, oral or electronic communication, knowing or  
 16 having reason to know that the information was obtained through the  
 17 interception of a wire, oral or electronic communication in violation  
 18 of this section;  
 19                   (iv) Use or attempt to use the contents of any wire, oral or  
 20 electronic communication knowing or having reason to know that the  
 21 information was obtained through the interception of a wire, oral or  
 22 electronic communication in violation of this section . . . .

23                  *See also Wyo. Stat. § 7-3-701(a)(v) (defining “electronic communication”).*

24                  Defendants Carrier IQ and the Device Manufacturers, by way of their  
 25 programming, knowing and intentional installation, activation, and other  
 26 involvement with the Carrier IQ Software, consisting of the IQ Agent and CIQ  
 27 Interface, have intentionally intercepted, endeavored to intercept, and/or have aided,  
 28 authorized, employed, or procured or permitted others to so do.

29                  Wyo. Stat. § 7-3-710 provides in pertinent part:

- 30                  (a) Subject to W.S. 7-3-702(b)(ii), any person whose wire,  
 31 oral or electronic communication is intercepted, disclosed or used in  
 32 violation of this act may recover damages against any person who  
 33 intercepts, discloses, uses or procures any other person to intercept,  
 34 disclose or use the communications as follows:  
 35                   (i) Actual damages but not less than one thousand dollars  
 36 (\$1,000.00) a day for each day of violation;  
 37                   (ii) Punitive damages; and  
 38                   (iii) Reasonable attorney's fees and other litigation costs  
 39 reasonably incurred.

Based on the allegations herein, plaintiffs and the class are entitled to the maximum damages provided by the foregoing statute, including punitive damages; and a reasonable attorney's fee and other litigation costs reasonably incurred.

114. Investigation regarding disclosures, including intentional disclosures, of the communications, content, information, and data referenced herein, or the endeavoring to disclose, intentionally or otherwise, the communications, content, information, and data referenced herein, is ongoing. Such activity may be actionable under all or some of the state statutes that follow.

**COUNT III**

**VIOLATION OF STATE CONSUMER PROTECTION ACTS**

(Against Carrier IQ and the Device Manufacturers)

(On Behalf of Residents of the States of Arkansas, California, Connecticut, Delaware, Florida, Hawaii, Kansas, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, Oklahoma, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Washington, and West Virginia)

115. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

116. Plaintiffs bring these claims on behalf of themselves and other owners of affected devices who reside in the states of Arkansas, California, Connecticut, Delaware, Florida, Hawaii, Kansas, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, Oklahoma, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Washington, and West Virginia. By the conduct and omissions described herein, defendants Carrier IQ and the Device Manufacturers have violated state consumer protection acts.

117. For example, in violation of California Business and Professions Code Sections 17200, *et seq.* (“UCL”), defendants’ conduct in this regard includes unlawful, unfair, and fraudulent business acts or practices. By engaging in the acts and practices described herein, defendants have committed one or more acts of unfair competition within the meaning of the UCL.

118. First, defendants' business acts and practices are unlawful under the UCL and similar state statutes in part because they violate the Federal Wiretap Act and California Penal Code §§ 502, 631, and 632.7. Additionally, HTC's conduct with respect to the logging issue described herein, per the FTC's Complaint and Final Decision and Order, violated the FTC Act, such that those business acts and practices also violated the UCL.

1           119. Second, defendants' business acts and practices are unfair because they caused harm  
 2 and injury-in-fact to plaintiffs and prospective class members without justification. Defendants'  
 3 conduct lacks reasonable and legitimate justification in that defendants have benefited from such  
 4 conduct and practices while plaintiffs and prospective class members have been misled as to the  
 5 nature and integrity of defendants' goods and services and have, in fact, suffered injury regarding  
 6 the privacy and confidentiality of their personal information and the use of their device resources.  
 7 Further, defendants' conduct is unfair because it offends California public policy as reflected in the  
 8 right to privacy enshrined in the state constitution; California Penal Code §§ 502, 631, and 632.7;  
 9 and California statutes recognizing the need for consumers to safeguard their privacy interests,  
 10 including California Civil Code § 1798.80. Defendants' business acts and practices also were  
 11 unfair in that defendants knew that consumers care deeply about personal, private, confidential, and  
 12 sensitive information, including data related to visited websites; search (including search terms),  
 13 user name, and password data; fine location data, including granular GPS data; application  
 14 purchases (including applications that could reveal a consumer's health conditions or sexual  
 15 orientation, among other private information) and uses; and text-message privacy (including  
 16 consumers' expectations that the content of their text messages would not be intercepted or sent to  
 17 anyone beyond the recipient for outgoing texts or themselves for incoming texts), yet they hid  
 18 software on their mobile devices that intercepted that data and transmitted most of it off of their  
 19 devices.

20           120. Third, defendants' acts and practices were fraudulent within the meaning of the  
 21 UCL because they were likely to mislead consumers. Defendants secretly installed the Carrier IQ  
 22 Software on plaintiffs' and prospective class members' mobile devices; failed to disclose that the  
 23 Carrier IQ Software was always operating on such devices; failed to disclose that the Carrier IQ  
 24 Software was capable of intercepting private communications, and that it in fact did intercept such  
 25 communications; and failed to disclose that the Carrier IQ Software degraded the performance of  
 26 their devices by overtaxing processor power and device memory, and by depleting battery power  
 27 and life. Defendants' omissions and failures to disclose were material to plaintiffs and the  
 28 prospective class within the meaning of *In re Tobacco II Cases*, 46 Cal. 4th 298, 325 (2009).

1           121. In addition, HTC failed to disclose with respect to its devices that plaintiffs' and  
 2 prospective class members' personal, private, confidential, and sensitive data was being logged in  
 3 unencrypted form on their devices, transmitted to third-parties including Google, itself via its "Tell  
 4 HTC" software, and likely application developers and vendors, including via the ACRA tool  
 5 available to application developers and vendors, which allowed them to access material in the  
 6 devices' system logs, and rendered vulnerable to malicious outsiders or anyone with access to the  
 7 debug logs on their devices.

8           122. Defendants had a duty to disclose the presence and functionality of the Carrier IQ  
 9 Software on the plaintiffs' and the prospective class' mobile devices. This duty was based on the  
 10 fact that only defendants knew of the installation and functionality of the Carrier IQ Software on  
 11 the plaintiffs' and prospective class' mobile devices, and defendants knew that the existence of the  
 12 Carrier IQ Software was not known or reasonably discoverable by plaintiffs and the class. Further,  
 13 defendants actively concealed discovery of the Carrier IQ Software from plaintiffs by the very  
 14 design of the Carrier IQ Software and the method of installation on plaintiffs' mobile devices.  
 15 Indeed, as rootkit software, Carrier IQ Software was designed to be undetectable.

16           123. Defendants knew they were concealing the material facts regarding Carrier IQ  
 17 Software, and the effect concealment of those facts would have, and intended to induce plaintiffs'  
 18 and the class members' reliance.

19           124. Plaintiffs and the class did, in fact, rely on defendants' omissions of material facts  
 20 when they purchased their mobile devices. Such reliance was reasonable and justifiable under the  
 21 circumstances.

22           125. As a direct and proximate result of defendants' business acts or practices, plaintiffs  
 23 and class members were injured and damaged by being forced to relinquish - without informed  
 24 consent or critical knowledge - the purchase prices of their mobile devices. But for these unlawful,  
 25 unfair, and fraudulent business acts and practices, which hid from them the installation of the  
 26 Carrier IQ Software on their devices and its attributes and functions as described herein, plaintiffs  
 27 and prospective class members would never have purchased their mobile devices. Accordingly,

1 each plaintiff and prospective class member is entitled to restitution in the form of a purchase price  
 2 refund from the Device Manufacturer of his or her mobile device. Cal. Bus. & Prof. Code § 17203.

3       126. In addition, or in the alternative, plaintiffs and prospective class members are  
 4 entitled to injunctive relief against Carrier IQ and the Device Manufacturers to prevent the  
 5 admitted interception or capture and transmittal of URLs containing HTTP and HTTPS strings that  
 6 include search terms and sensitive information such as user names and passwords, dialer-pad  
 7 keypresses, as well as personalized geo-location information. Cal. Bus. & Prof. Code § 17203.

8       127. Also, or in the alternative, if not already completed in response to HTC's agreement  
 9 with the FTC, which was entered into following the filing of the First Consolidated Amended  
 10 Complaint, plaintiffs and prospective class members with HTC mobile devices running on the  
 11 Android OS are entitled to injunctive and other equitable relief against HTC and Carrier IQ to  
 12 remedy any continuing copying of the foregoing information, as well as SMS text message content,  
 13 to system logs, which are being transmitted off-device to Google, to HTC itself via its Tell HTC  
 14 software, and likely to third-party application developers without authorization, and whose logging  
 15 creates extreme vulnerability to capture by malicious means. Cal. Bus. & Prof. Code § 17203.

16       128. Further, defendants have violated California Civil Code section 1710(3) by  
 17 suppressing and/or failing to disclose facts that they were bound to disclose.

18       129. Finally, plaintiffs and the prospective class are entitled to recover their attorneys'  
 19 fees because by way of this lawsuit, they seek to enforce important rights affecting the public  
 20 interest, and because they otherwise satisfy the statutory requirements for an award of attorneys'  
 21 fees. Cal. Code Civ. P. § 1021.5.

22       130. Furthermore - as a result of defendants' actions, omissions, and willful, unlawful,  
 23 unfair, unconscionable, or fraudulent conduct as described above, which descriptions are  
 24 incorporated here by this reference, plaintiffs and owners of affected devices who reside in other  
 25 states are likewise entitled to similar damages, including multiple or exemplary or punitive  
 26 damages as permitted, and injunctive or other equitable relief as described above, as well as  
 27 attorneys' fees and costs, under the consumer protection acts of their home states. Accordingly,

plaintiffs allege as follows, on behalf of the plaintiffs and class members domiciled or who purchased mobile devices in each respective state:

**ARKANSAS**  
**VIOLATION OF THE ARKANSAS DECEPTIVE TRADE PRACTICES ACT**  
**(Ark. Code Ann. § 4-88-107(a)(10).)**

131. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

132. The Arkansas Deceptive Trade Practices Act (“DTPA”) prohibits “deceptive and unconscionable trade practices,” which include but are not limited to a list of enumerated items, including “[e]ngaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade[.]” Ark. Code Ann. § 4-88-107(a)(10).

133. Defendants are “persons” within the meaning of the DTPA. Ark. Code Ann. § 4-88-102(5).

134. The conduct of defendants as set forth herein constitutes deceptive and unconscionable trade practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and their misrepresentations and omissions regarding the privacy and functionality of their mobile devices also constitute unconscionable or deceptive trade practices.

135. Defendants' conduct was unconscionable because it affronts the sense of justice decency or reasonableness, including as established by public policy and the state and federal privacy laws enumerated herein. Defendants' unconscionable and deceptive trade practices occurred or were committed in the course, vocation or occupation of defendants' business, commerce, or trade. Defendants are each directly liable for these violations of law.

136. Defendants engaged in a deceptive trade practice when they failed to disclose material information concerning the mobile devices which was known to defendants at the time of the sale. Defendants deliberately concealed, suppressed, or omitted information about the mobile devices' the Carrier IQ Software and its interception and transmission of private information and data, intending that consumers would rely on that omission, in order to ensure that consumers would purchase their mobile devices.

137. The information withheld was material in that it was information that was important to consumers and likely to affect their choice of, or conduct regarding, the purchase of their mobile devices. Defendants' withholding of this information was likely to mislead consumers acting reasonably under the circumstances. The propensity of the mobile devices with the Carrier IQ Software installed to intercept and transmit private information and data was material to plaintiffs and the class. Had plaintiffs and the class known that their mobile devices had these serious privacy defects, they would not have purchased their mobile devices.

138. Defendants' conduct proximately caused injuries to plaintiffs and the class.

139. Plaintiffs and the class were injured as a result of defendants' conduct in that plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices are materially different than what was bargained for, and have also suffered a diminution in value. These injuries are the direct and natural consequence of defendants' unconscionable conduct, misrepresentations and omissions.

140. Plaintiffs are entitled to recover actual damages, as well as reasonable attorneys' fees, for defendants' unlawful conduct.

**CONNECTICUT**  
**VIOLATION OF CONNECTICUT UNLAWFUL TRADE PRACTICES ACT**  
**(Conn. Gen. Stat. § 42-110A, *et seq.*)**

141. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

142. The Connecticut Unfair Trade Practices Act (“CUTPA”) provides: “No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Conn. Gen. Stat. § 42- 110b(a).

1           143. Defendants are persons within the meaning of the CUTPA. Conn. Gen. Stat. § 42-  
 2         110a(3).

3           144. In the course of defendants' business, they designed and installed the Carrier IQ  
 4         Software on mobile devices as described above, and then caused those mobile devices to be sold to  
 5         consumers, including plaintiffs. This caused the interception and transmission of private  
 6         information and data in violation of several state and federal laws, as alleged herein.

7           145. Defendants' conduct was unfair because it offends established public policy, is  
 8         immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,  
 9         including by violation of the state and federal privacy laws enumerated herein.

10          146. The presence and functionality of the Carrier IQ Software on the mobile devices,  
 11         including the interception and transmission of private information and data, was not disclosed to  
 12         plaintiffs, but was information considered material by plaintiffs and the class. Had plaintiffs and  
 13         the class known that their mobile devices had these serious privacy defects, they would not have  
 14         purchased their mobile devices.

15          147. Plaintiffs and the class accordingly suffered ascertainable loss caused by  
 16         defendants' deceptive and unfair practices. Plaintiffs and the class overpaid for their mobile  
 17         devices and did not receive the benefit of their bargain. The value of their mobile devices have  
 18         diminished now that the privacy issues have come to light, and plaintiffs and the class purchased  
 19         mobile devices that are not secure and private. Further, the secretly installed Carrier IQ Software  
 20         embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by  
 21         causing slower performance and decreased battery life. The harm caused to plaintiffs and the class  
 22         greatly outweighs any associated benefit.

23          148. Plaintiffs are entitled to recover their actual damages, punitive damages, and  
 24         attorneys' fees pursuant to Conn. Gen. Stat. § 42-110g.

25          149. Pursuant to Conn. Gen. Stat. § 42-110g(c), plaintiffs will mail a copy of this  
 26         complaint to Connecticut's Attorney General.

**DELAWARE**  
**VIOLATION OF THE DELAWARE CONSUMER FRAUD ACT**  
**(6 Del. Code § 2513, et seq.)**

150. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

151. The Delaware Consumer Fraud Act prohibits the “act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale, use or advertisement of any merchandise, whether or not any person has in fact been misled, deceived or damaged thereby.”<sup>6</sup> Del. Code § 2513(a).

152. Defendants are persons with the meaning of 6 Del. Code § 2511(7).

153. As described herein defendants concealed, suppressed, or omitted material facts regarding the privacy and functionality of their mobile devices and the Carrier IQ Software installed on those mobile devices, including that their mobile devices, with the Carrier IQ Software installed, would intercept and transmit private information and data to third parties, and the fact that those mobile devices suffer slower performance and reduced battery life as a result of the Carrier IQ Software. Defendants intended that others rely on these misrepresentations and omissions in connection with the sale and use of their mobile devices.

154. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

155. Defendants' conduct proximately caused injuries to plaintiffs and the class.

156. Plaintiffs and the class were injured as a result of defendants' conduct in that plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices have suffered a diminution in value. These injuries are the direct and natural consequence of defendants' misrepresentations and omissions.

157. Plaintiffs are entitled to recover damages, as well as punitive damages, for defendants' gross and aggravated misconduct.

1

**FLORIDA**  
**VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT**  
**(Fla. Stat. § 501.201, *et seq.*)**

2

3       158. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

4       159. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or  
 5 practices, including, but not limited to defendants' design and installation of the Carrier IQ  
 6 Software on mobile devices as described above, which causes the mobile devices to intercept and  
 7 transmit private information and data to third parties. Defendants then caused those mobile devices  
 8 to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose  
 9 and remedy the problems inherent in the Carrier IQ Software.

10      160. Defendants' conduct was thus unfair because it offends established public policy, is  
 11 immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,  
 12 including by violation of the state and federal privacy laws enumerated herein.

13      161. Defendants' actions as set forth above occurred in the conduct of trade or  
 14 commerce.

15      162. Defendants' actions impact the public interest because plaintiffs were injured in  
 16 exactly the same way as millions of others purchasing and/or using mobile devices as a result of  
 17 Defendants' generalized course of unfair conduct and deception. All of the wrongful conduct  
 18 alleged herein occurred, and continues to occur, in the conduct of defendants' business.

19      163. Plaintiffs and the class were injured as a result of defendants' conduct.

20      164. Plaintiffs overpaid for their mobile devices and did not receive the benefit of their  
 21 bargain, and their mobile devices have suffered a diminution in value. Further, the secretly  
 22 installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those  
 23 mobile devices, causing slower performance and decreased battery life.

24      165. Defendants' conduct proximately caused the injuries to plaintiffs and the class.

25      166. Defendants are liable to plaintiffs and the class for damages in amounts to be proven  
 26 at trial, including attorneys' fees, costs, and treble damages.

**HAWAII  
UNFAIR COMPETITION AND PRACTICES  
(Haw. Rev. Stat. § 480, *et seq.*)**

167. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

168. Hawaii's Revised Statute § 480-2(a) prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce...."

169. Defendants' conduct as set forth herein constitutes unfair methods of competition and unfair or deceptive acts or practices in violation of Haw. Rev. Stat. § 480-2 because defendants' acts and practices, including (1) the design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties and causes decreased battery life and slower performance in those mobile devices, (2) defendants' failure to adequately investigate, disclose and remedy the problem, (3) defendants' sale of mobile devices containing the Carrier IQ Software directly to consumers, or to distributors and third parties, with the intent that consumers, including plaintiffs, would purchase those mobile devices, and (4) defendants' misrepresentations and omissions regarding the privacy and functionality of their mobile devices, offend established public policy, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein. The harm defendants have caused to consumers greatly outweighs any benefits associated with those practices. Defendants' conduct has also prevented plaintiffs from making fully informed decisions about whether to purchase or use mobile devices and/or the price to be paid to purchase or use mobile devices.

170. Had plaintiffs known the true facts about the privacy and functionality of their mobile devices, they would not have purchased or used, or paid as much for, the mobile devices.

171. Defendants' acts or practices as set forth above occurred in the conduct of trade or commerce.

172. Plaintiffs and the class have suffered injury, including the loss of money or property, as a result of defendants' unfair methods of competition and unfair or deceptive acts or practices.

173. In addition to damages in amounts to be proven at trial, plaintiffs and the class seek attorneys' fees, costs of suit and treble damages.

174. Plaintiffs and the class also seek injunctive relief to enjoin defendants from continuing their unfair competition and unfair or deceptive acts or practices.

**KANSAS**  
**VIOLATIONS OF THE KANSAS CONSUMER PROTECTION ACT**  
**(Kan. Stat. Ann. § 50-623, et seq.)**

175. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

176. Defendants are “suppliers” under § 50-624(l) of the Kansas Consumer Protection Act (“Kansas CPA”).

177. Plaintiffs are “consumers,” as defined by § 50-624(b) of the Kansas CPA, who purchased or used one or more mobile devices.

178. Defendants participated in deceptive acts or practices that violated the Kansas CPA, as described above and below. Defendants each are directly liable for these violations of law.

179. Defendants engaged in deceptive acts or practices prohibited by the Kansas CPA by willfully failing to disclose or willfully concealing, suppressing, or omitting material facts about their mobile devices and the Carrier IQ Software they designed and installed on those mobile devices. Specifically, defendants failed to disclose and actively concealed the fact that the mobile devices would cause interception and transmission of private information and data. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life, which fact the defendants also failed to disclose and actively concealed. Defendants nevertheless failed to warn plaintiffs and the class about these inherent dangers despite having a duty to do so.

180. Whether or not a mobile device (a) intercepts private information and data and (b) transmits private information and data to third parties are facts that a reasonable consumer would consider important in selecting a mobile device to purchase or use. When plaintiffs bought a mobile device for personal, family, or household purposes, they reasonably expected the mobile

device would (a) not intercept private information and data; and (b) not transmit private information and data to third parties.

181. Defendants' deceptive and unconscionable acts or practices were likely to and did in fact deceive reasonable consumers, including plaintiffs, about the true privacy and functionality of mobile devices as a result of defendants' violations of the Kansas CPA.

182. Plaintiffs and the class suffered loss as a result of defendants' violations of the Kansas CPA detailed above. Plaintiffs currently own or use, or within the class period have owned or used, mobile devices that are defective and inherently lacking in privacy protections. The Carrier IQ Software and the resulting interception and transmission of private information and data to third parties have caused the value of mobile devices to plummet. Plaintiffs would not have purchased their mobile devices, or would have paid significantly less for them, had they known of the Carrier IQ Software and its functionality.

183. Pursuant to § 50-634(b) of the Kansas CPA, plaintiffs seek monetary relief against defendants measured as the greater of (a) actual damages in an amount to be determined at trial and (b) civil penalties provided for by § 50-636 of the Kansas CPA.

184. Plaintiffs risk irreparable injury as a result of defendants' deceptive and unconscionable acts or practices in violation of the Kansas CPA, and these violations present a continuing risk to plaintiffs, their friends, family, and acquaintances, and the general public.

185. Plaintiffs and the class further seek an order enjoining defendants' deceptive and unconscionable acts or practices, restitution, punitive damages, costs of court, attorneys' fees, and any other just and proper relief available under the Kansas CPA.

**MARYLAND**  
**VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT**  
**(Md. Code Com. Law § 13-101, et seq.)**

186. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

187. Plaintiffs are persons within the meaning of the Maryland Consumer Protection Act (the “Act”) for all purposes therein.

188. Defendants are persons within the meaning of the Act for all purposes therein.

1           189. Defendants' conduct was unfair because it offends established public policy, is  
 2 immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,  
 3 including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair  
 4 and deceptive trade practices occurred or were committed in the course, vocation or occupation of  
 5 defendants' businesses. Defendants are each directly liable for these violations of law.

6           190. The Unfair and Deceptive Trade Practices as alleged above and below significantly  
 7 impact the public as actual or potential customers of defendants.

8           191. By designing and installing the Carrier IQ Software on mobile devices, and then  
 9 causing those mobile devices to be sold to plaintiffs, as well as failing to disclose and actively  
 10 concealing the potential for interception and transmission of private information and data in mobile  
 11 devices equipped with the IQ Agent, defendants engaged in unfair business practices prohibited by  
 12 the Act.

13           192. As a direct and proximate result of their unfair and deceptive business practices, and  
 14 violations of the Act detailed above, defendants caused actual damages, injuries, and losses to  
 15 plaintiffs and, if not stopped, will continue to harm plaintiffs. Plaintiffs currently own or use, or  
 16 within the class period have owned or used, mobile devices that are defective and inherently  
 17 lacking in privacy protections. Further, the secretly installed Carrier IQ Software embedded on  
 18 plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower  
 19 performance and decreased battery life. The Carrier IQ Software and its interception and  
 20 transmission of private information and data, as well as its causing slower performance and  
 21 reduced battery life, have caused the value of mobile devices to plummet.

22           193. Plaintiffs are entitled to all damages permitted by Md. Code Com. Law § 13-101, *et*  
 23 *seq.*, including actual damages sustained, civil penalties, attorneys' fees, and costs of this action.  
 24 Also, the State of Maryland is entitled to statutory penalties from defendants for each violation of  
 25 the Act.

**MICHIGAN**  
**VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT**  
**(Mich. Comp. Laws § 445.901, et seq.)**

194. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

195. The Michigan Consumer Protection Act prohibits “[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.” Mich. Comp. Laws § 445.903.

196. Defendants engaged in unfair, unconscionable, or deceptive acts or practices prohibited by the Michigan Consumer Protection Act when they failed to reveal material facts regarding their mobile devices and the Carrier IQ Software they designed and installed on those mobile devices. Specifically, defendants failed to reveal the fact that the Carrier IQ Software installed on their mobile devices would cause interception and transmission of private information and data, as well as reduced performance and diminished battery life. Defendants nevertheless failed to warn plaintiffs and the class about these inherent defects despite having a duty to do so.

197. Whether or not a mobile device (a) intercepts private information and data and (b) transmits private information and data to third parties are facts that a reasonable consumer would consider important in selecting a mobile device to purchase or use. When plaintiffs bought a mobile device, they reasonably expected the mobile device would (a) not intercept private information and data; and (b) not transmit private information and data to third parties.

198. The Michigan Consumer Protection Act applies to defendants' transactions with plaintiffs because defendants' deceptive scheme was carried out in Michigan and affected plaintiffs.

199. Defendants also failed to advise the public about what they knew about the Carrier IQ Software, which causes the mobile devices to intercept and transmit private information and data to third parties.

200. A reasonable person would have relied on defendants' silence as to known defects in connection with their decision regarding the purchase, use and/or use of the mobile devices.

201. As a direct and proximate result of defendants' deceptive conduct and violation of the Michigan Consumer Protection Act, plaintiffs have sustained and will continue to sustain

economic losses and other damages for which they are entitled to compensatory damages and equitable and declaratory relief in an amount to be proven at trial. Plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices have suffered a diminution in value.

**MISSOURI**  
**VIOLATION OF MISSOURI MERCHANDISING PRACTICES ACT**  
**(Mo. Rev. Stat. § 407.010, et seq.)**

202. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

203. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and their misrepresentations and omissions regarding the privacy and functionality of their mobile devices also constitute unfair or deceptive practices.

204. Defendants' conduct was unfair because it offends established public policy, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein.

205. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

206. Defendants' actions impact the public interest because plaintiffs were injured in exactly the same way as millions of others purchasing and/or using mobile devices as a result of defendants' generalized course of unfair conduct. All of the wrongful conduct alleged herein occurred, and continues to occur, in the conduct of defendants' business.

207. Plaintiffs and the class were injured as a result of defendant's conduct. Plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile

devices have suffered a diminution in value. This diminution in value amounts to an ascertainable loss of money.

208. Defendants' conduct proximately caused the injuries to plaintiffs and the class.

209. Defendants are liable to plaintiffs and the class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

210. Pursuant to Mo. Rev. Stat. § 407.010, plaintiffs will serve the Missouri Attorney General with a copy of this complaint as plaintiffs seek injunctive relief

**NEVADA**  
**VIOLATION OF THE NEVADA DECEPTIVE TRADE PRACTICES ACT**  
**(Rev. Stat. § 598.0903, *et seq.*)**

211. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

212. Defendants are “persons” as required under the statute.

213. Defendants' actions as set forth above occurred in the course of business.

214. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0903, *et seq.*, prohibits unfair or deceptive consumer sales practices.

215. The Nev. Rev. Stat. § 598.0915 provides that a person engages in a “deceptive trade practice” if, in the course of his or her business or occupation, he or she does any of the following, including, *inter alia*, “1. Knowingly fails to disclose a material fact in connection with the sale or lease of goods or services.” Nev. Rev. Stat. § 598.0923(2)

216. In the course of defendants' business, they knowingly failed to disclose material facts regarding their design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties, as well as reduced battery life and slower performance. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the problems inherent in the Carrier IQ Software.

217. The information withheld was material in that it was information that was important to consumers and likely to affect their choice of, or conduct regarding, the purchase of their mobile devices. Defendants' withholding of this information was likely to mislead consumers acting

reasonably under the circumstances. The propensity of the mobile devices with the Carrier IQ Software installed to intercept and transmit private information and data was material to plaintiffs and the class. Had plaintiffs and the class known that their mobile devices had these serious privacy defects, they would not have purchased their mobile devices.

218. Plaintiffs and the class suffered ascertainable loss caused by defendants' false representations and failure to disclose material information. Plaintiffs and the class overpaid for their mobile devices and did not receive the benefit of their bargain. The value of their mobile devices has diminished now that the privacy issues have come to light, and plaintiffs and the class purchased mobile devices that are not secure and are less valuable than what was promised them.

**NEW HAMPSHIRE**  
**VIOLATION OF N.H. CONSUMER PROTECTION ACT**  
**(N.H. Rev. Stat. Ann. § 358A:1, *et seq.*)**

219. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

220. The New Hampshire Consumer Protection Act (“CPA”) prohibits a person, in the conduct of any trade or commerce, from engaging in “any unfair or deceptive act or practice in the conduct of any trade or commerce within this state” .” N.H. Rev. Stat. § 358-A:2.

221. Defendants are persons within the meaning of the CPA. *See* N.H. Rev. Stat. § 358A:1(I).

222. In the course of defendants' business, they designed and installed the Carrier IQ Software on mobile devices, caused those mobile devices to be sold to consumers, including plaintiffs, and willfully failed to disclose and actively concealed the potential for interception and transmission of private information and data in mobile devices equipped with the Carrier IQ Software as described above. Accordingly, defendants engaged in unfair and unlawful acts.

223. Defendants' conduct was unfair because it offends established public policy, violates or offends state and federal statutory and common law, or falls within the penumbra of those laws, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein.

224. The propensity of the mobile devices with the Carrier IQ Software installed to intercept and transmit private information and data were material to plaintiffs and the class. Had plaintiffs and the class known that their mobile devices had these serious privacy defects, they would not have purchased their mobile devices.

225. Defendants' unfair and deceptive acts or practices, including their failure to disclose material information, has injured plaintiffs and the class. Plaintiffs and the class overpaid for their mobile devices and did not receive the benefit of their bargain. The value of their mobile devices has diminished now that the privacy issues have come to light, and plaintiffs and the class purchased mobile devices that are not secure, and suffer reduced performance and battery life.

226. Plaintiffs are entitled to recover the greater of actual damages or \$1,000 pursuant to N.H. Rev. Stat. § 358-A:10. Plaintiffs are also entitled to treble damages because defendants acted willfully in their unfair and deceptive practices.

**NEW JERSEY**  
**VIOLATION OF NEW JERSEY CONSUMER FRAUD ACT**  
**(N.J. Stat. Ann. § 56:8-1, et seq.)**

227. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

228. The New Jersey Consumer Fraud Act (“CFA”) makes unlawful “[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby...” N.J. Stat. Ann. § 56:8-2.

<sup>229.</sup> Defendants are persons within the meaning of the CFA. N.J. Stat. Ann. § 56:8-1(d).

230. Defendants engaged in an unlawful practice under the CFA when, in the course of defendants' business, they knowingly failed to disclose and actively concealed their design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties, as well as reduced battery life and slower performance.

231. Defendants deliberately withheld the information about the mobile devices' the Carrier IQ Software and its interception and transmission of private information and data in order to ensure that consumers would purchase their mobile devices and to induce the consumer to enter into a transaction.

232. Defendants' unlawful practices cause substantial injury to consumers.

233. Defendants' design and installation of the Carrier IQ Software, and the propensity of the mobile devices with the IQ Agent installed to intercept and transmit private information and data was material to plaintiffs and the class. Had plaintiffs and the class known that their mobile devices had these serious privacy defects, they would not have purchased their mobile devices.

234. Plaintiffs and the class suffered ascertainable loss of money or property caused by defendants' unlawful practices. Plaintiffs and the class overpaid for their mobile devices and did not receive the benefit of their bargain. The value of their mobile devices has diminished now that the privacy issues have come to light, and plaintiffs and the class purchased mobile devices that are not safe.

235. Plaintiffs are entitled to recover legal and/or equitable relief, treble damages, and reasonable attorneys' fees pursuant to N.J. Stat. Ann. § 56:8-19.

236. Pursuant to N.J. Stat. Ann. § 56:8-20, plaintiffs will mail a copy of the complaint to New Jersey's Attorney General within ten (10) days of filing it with the Court.

**OKLAHOMA**  
**VIOLATION OF OKLAHOMA CONSUMER PROTECTION ACT**  
**(Okla. Stat. tit. 15 § 751, *et seq.*)**

237. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

238. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants then caused those

1 mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately  
 2 investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and  
 3 their misrepresentations and omissions regarding the privacy and functionality of their mobile  
 4 devices also constitute unfair or deceptive practices.

5 239. Defendants' conduct was unfair because it offends established public policy, is  
 6 immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,  
 7 including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair  
 8 and deceptive trade practices occurred or were committed in the course, vocation or occupation of  
 9 defendants' businesses. Defendants are each directly liable for these violations of law.

10 240. Defendants' actions as set forth above occurred in the conduct of trade or  
 11 commerce.

12 241. Defendants' actions impact the public interest because plaintiffs were injured in  
 13 exactly the same way as millions of others purchasing and/or using mobile devices as a result of  
 14 defendants' generalized course of unfair conduct and deception. All of the wrongful conduct  
 15 alleged herein occurred, and continues to occur, in the conduct of defendants' business.

16 242. Plaintiffs and the class were injured as a result of defendants' conduct. Plaintiffs  
 17 overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile  
 18 devices have suffered a diminution in value.

19 243. Defendants' conduct proximately caused the injuries to plaintiffs and the class.

20 244. Defendants are liable to plaintiffs and the class for damages in amounts to be proven  
 21 at trial, including attorneys' fees, costs, and treble damages.

22 245. Pursuant to Okla. Stat. tit. 15 § 751, plaintiffs will serve the Oklahoma Attorney  
 23 General with a copy of this complaint as plaintiffs seek injunctive relief.

24  
 25  
 26  
 27  
 28

**RHODE ISLAND**  
**VIOLATION OF THE RHODE ISLAND UNFAIR TRADE PRACTICES**  
**AND CONSUMER PROTECTION ACT**  
**(R.I. Gen. Laws § 6-13.1, *et seq.*)**

246. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

247. Plaintiffs are persons who purchase or use goods primarily for personal, family, or household purposes within the meaning of R.I. Gen. Laws § 6- 13.1-5.2(a).

248. Rhode Island's Unfair Trade Practices and Consumer Protection Act ("UTPCPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce" including:

"(v) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have"; "(vii) Representing that goods or services are of a particular standard, quality, or grade ... , if they are of another"; "(ix) Advertising goods or services with intent not to sell them as advertised"; "(xii) Engaging in any other conduct that similarly creates a likelihood of confusion or of misunderstanding"; "(xiii) Engaging in any act or practice that is unfair or deceptive to the consumer"; and "(xiv) Using any other methods, acts or practices which mislead or deceive members of the public in a material respect." R.I. Gen. Laws § 6-13.1-1(6).

249. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ, and their misrepresentations and omissions regarding the privacy and functionality of their mobile devices also constitute unfair or deceptive practices.

250. Defendants' conduct was unfair because it offends established public policy, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,

including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair and deceptive trade practices occurred or were committed in the course, vocation or occupation of defendants' businesses. Defendants are each directly liable for these violations of law.

251. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

252. Plaintiffs suffered ascertainable loss of money as a result of defendants' violation of the UTPCPA.

253. Plaintiffs and the class were injured as a result of defendants' conduct in that plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices have suffered a diminution in value. These injuries are the direct and natural consequence of defendants' misrepresentations and omissions.

254. Accordingly, plaintiffs and the class are entitled to recover the greater of actual damages or \$200 pursuant to R.I. Gen. Laws § 6-13.1-5.2(a).

**SOUTH CAROLINA**  
**VIOLATIONS OF THE SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT**  
**(S.C. Code Ann. § 39-5-10, et seq.)**

255. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

256. Defendants are “persons” under S.C. Code Ann. § 39-5-10.

257. Defendants participated in unfair or deceptive acts or practices that violated the South Carolina Unfair Trade Practices Act (the “Act”), S.C. Code Ann. § 39-5-10, *et seq.*, as described above and below. Defendants each are directly liable for these violations of law.

258. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately

1 investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and  
 2 their misrepresentations and omissions regarding the privacy and functionality of their mobile  
 3 devices also constitute unfair or deceptive practices.

4       259. Defendants' conduct was unfair because it offends established public policy, is  
 5 immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers,  
 6 including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair  
 7 and deceptive trade practices occurred or were committed in the course, vocation or occupation of  
 8 defendants' businesses. Defendants are each directly liable for these violations of law.

9       260. Defendants knew that the Carrier IQ Software in their mobile devices was  
 10 defectively designed, installed, or manufactured, and caused the mobile devices to intercept and  
 11 transmit private information and data. Defendants nevertheless failed to warn plaintiffs about these  
 12 inherent defects despite having a duty to do so.

13       261. Defendants each owed plaintiffs a duty to disclose the defective nature of mobile  
 14 devices, including the serious privacy violations caused by the Carrier IQ Software because they:

- 15           (a) Possessed exclusive knowledge of the defects rendering the mobile devices containing  
                  the Carrier IQ Software inherently more susceptible to serious privacy violations than  
                  similar mobile devices; and
- 16           (b) Made incomplete representations about the privacy and functionality of mobile devices  
                  generally, and the Carrier IQ Software in particular, while purposefully withholding  
                  material facts from plaintiffs that contradicted these representations.

21       262. Mobile devices equipped with the Carrier IQ Software pose an unreasonable risk of  
 22 serious privacy violations to plaintiffs, their friends and family, and the public at large, because  
 23 they are susceptible to interception and transmission of private information and data.

24       263. Whether or not a mobile device (a) intercepts private information and data and (b)  
 25 transmits private information and data to third parties are facts that a reasonable consumer would  
 26 consider important in selecting a mobile device to purchase or use.

264. When plaintiffs bought a mobile device for personal, family, or household purposes, they reasonably expected the mobile device would (a) not intercept private information and data; and (b) not transmit private information and data to third parties.

265. Defendants' unfair or deceptive trade practices were likely to and did in fact deceive reasonable consumers, including plaintiffs, about the true privacy and functionality of mobile devices.

266. As a result of their violations of the Act detailed above, defendants caused actual damage to plaintiffs and, if not stopped, will continue to harm plaintiffs. Plaintiffs currently own or use, or within the class period have owned or used, mobile devices that are defective and inherently lacking in privacy protections. The Carrier IQ Software and the resulting interceptions, transmissions, and other privacy violations have caused the value of plaintiffs' mobile devices to plummet.

267. Plaintiffs risk irreparable injury as a result of defendants' acts and omissions in violation of the Act, and these violations present a continuing risk to plaintiffs as well as to the general public.

268. Pursuant to S.C. Code Ann. § 39-5-140, plaintiffs seek monetary relief against defendants to recover for their sustained losses.

269. Plaintiffs further seek an order enjoining defendants' unfair or deceptive acts or practices, restitution, punitive damages, costs of court, attorneys' fees, and any other just and proper relief available under the Act.

**SOUTH DAKOTA  
VIOLATION OF THE SOUTH DAKOTA  
DECEPTIVE TRADE PRACTICES ACT  
(S.D. Codified Laws § 37-24-6)**

270. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

271. South Dakota law makes it unlawful for any person to engage in a “deceptive act or practice,” including “[k]nowingly and intentionally act, use or employ any deceptive act or practice . . . or to conceal, suppress, or omit any material fact in connection with the sale or advertisement

of any merchandise, regardless of whether any person has in fact been misled, deceived, or damaged thereby[.]” S.D. Codified Laws § 37-24-6(1).

272. Defendants are “persons” under the statue. S.D. Codified Laws § 37-24-6(8). The conduct of defendants as set forth herein constitutes deceptive acts or practices, including, but not limited to, defendants knowingly concealed, suppressed, or omitted material facts regarding their design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Defendants caused their mobile devices to be sold to consumers.

273. Plaintiffs and the class were injured as a result of defendants' conduct. Plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices have suffered a diminution in value.

274. Defendants' conduct proximately caused the injuries to plaintiffs and the class.

275. Under S.D. Codified Laws § 37-24-31, plaintiffs and the class are entitled to recovery of their actual damages suffered as a result of defendants' acts and practices.

**TEXAS**  
**VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT**  
**(Tex. Bus. & Com. Code §§ 17.41, et seq.)**

276. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

277. Defendants' above-described acts and omissions constitute false, misleading or deceptive acts or practices under the Texas Deceptive Trade Practices- Consumer Protection Act, Tex. Bus. & Com. Code § 17.41, et seq. ("Texas DTPA").

278. By failing to disclose and actively concealing the potential for interception and transmission of private information and data in mobile devices equipped with the Carrier IQ Software, defendants engaged in deceptive business practices prohibited by the Texas DTPA, including “failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the

1 consumer into a transaction into which the consumer would not have entered had the information  
 2 been disclosed.” Tex. Bus. & Com. Code § 17.46(b)(24).

3 279. Defendants’ unfair or deceptive acts or practices were likely to and did in fact  
 4 deceive reasonable consumers, including plaintiffs, about the true privacy and functionality of their  
 5 mobile devices.

6 280. In purchasing or using their mobile devices, the plaintiffs relied on the omissions of  
 7 defendants with respect to the privacy and functionality of the mobile devices. Defendants knew  
 8 that Carrier IQ Software was installed on their mobile devices, and knew of its functionality.  
 9 Nonetheless, defendants failed to disclose that their mobile devices contain Carrier IQ Software  
 10 which causes the phones to intercept and transmit private information and data from plaintiffs’  
 11 mobile devices, and causes the mobile devices to suffer slower performance and reduced battery  
 12 life. These facts were material to plaintiffs, as they are facts that plaintiffs would have considered  
 13 important at the time of purchase. Despite knowing these material facts, defendants failed to  
 14 disclose them to consumers and plaintiffs, with the intent that consumers and plaintiffs would be  
 15 induced to purchase their mobile devices. Had the plaintiffs known this, they would not have  
 16 purchased or used their mobile devices and/or paid as much for them.

17 281. Furthermore, because defendants took advantage of the consumers’ lack of  
 18 knowledge regarding the Carrier IQ Software to a grossly unfair degree, defendants have also  
 19 committed unconscionable acts or practices under § 17.50(a).

20 282. Defendants also breached express and implied warranties to plaintiffs and the class,  
 21 as set out herein, and are, therefore liable to plaintiffs and the class for damages under §§  
 22 17.50(a)(2) and 17.50(b) of the Texas DTPA. Defendants’ actions also constitute an  
 23 unconscionable action or course of action under § 17.50(a)(3) of the Texas DTPA.

24 283. Plaintiffs and the class sustained damages as a result of the defendants unlawful acts  
 25 and are, therefore, entitled to damages and other relief provided for under § 17.50(b) of the Texas  
 26 DTPA. Because defendants’ conduct was committed knowingly and/or intentionally, plaintiffs and  
 27 the class are entitled to treble damages.

284. For those plaintiffs and the class who wish to rescind their purchases, they are entitled under § 17.50(b)(4) to rescission and other relief necessary to restore any money or property that was acquired from them based on violations of the Texas DTPA.

285. Plaintiffs and the class also seek court costs and attorneys' fees under § 17.50(d) of the Texas DTPA.

**VERMONT**  
**VIOLATION OF VERMONT CONSUMER FRAUD ACT**  
**(Vt. Stat. Ann. tit. 9, § 2451, et seq.)**

286. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

287. The Vermont Consumer Fraud Act (“VCFA”) makes unlawful “[u]nfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce....” Vt. Stat. Ann. tit. 9, § 2453(a).

288. Defendants are sellers within the meaning of the VCFA. Vt. Stat. Ann. tit. 9, § 2451(a)(c).

289. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties, and causes slower performance and reduced battery life. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and their misrepresentations and omissions regarding the privacy and functionality of plaintiffs' mobile devices also constitute unfair or deceptive practices.

290. Defendants' conduct was unfair because it offends established public policy, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair and deceptive trade practices occurred or were committed in the course, vocation or occupation of defendants' businesses. Defendants are each directly liable for these violations of law. Defendants knew or should have known that their conduct violated the VCFA.

1           291. Defendants engaged in a deceptive trade practice under the VCFA when they failed  
 2 to disclose material information concerning the mobile devices which was known to defendants at  
 3 the time of the sale. Defendants deliberately withheld the information about the mobile devices'  
 4 Carrier IQ Software and its interception and transmission of private information and data in order  
 5 to ensure that consumers would purchase their mobile devices and to induce the consumer to enter  
 6 into a transaction.

7           292. The information withheld was material in that it was information that was important  
 8 to consumers and likely to affect their choice of, or conduct regarding, the purchase of their mobile  
 9 devices. Defendants' withholding of this information was likely to mislead consumers acting  
 10 reasonably under the circumstances. The propensity of the mobile devices with the Carrier IQ  
 11 Software installed to intercept and transmit private information and data was material to plaintiffs  
 12 and the class. Had plaintiffs and the class known that their mobile devices had these serious  
 13 privacy defects, they would not have purchased their mobile devices.

14           293. Defendants' conduct has caused or is to cause a substantial injury that is not  
 15 reasonably avoided by consumers, and the harm is not outweighed by a countervailing benefit to  
 16 consumers or competition.

17           294. Plaintiffs and the class have suffered injury and damages as a result of defendants'  
 18 false or fraudulent representations and unfair or deceptive practices in violation of Vt. Stat. Ann.  
 19 tit. 9, § 2453. Plaintiffs and the class overpaid for their mobile devices and did not receive the  
 20 benefit of their bargain. The value of their mobile devices has diminished now that the privacy  
 21 issues have come to light, and plaintiffs and the class purchased mobile devices that are not secure  
 22 and suffer from slower performance and reduced battery life.

23           295. Plaintiffs are entitled to recover "appropriate equitable relief" and "the amount of  
 24 [their] damages, or the consideration or the value of the consideration given by [them], reasonable  
 25 attorneys' fees, and exemplary damages not exceeding three times the value of the consideration  
 26 given by [them]" pursuant to Vt. Stat. Ann. tit. 9, § 2461(b).

**WASHINGTON**  
**VIOLATION OF THE CONSUMER PROTECTION ACT**  
**(Rev. Code Wash. Ann. § 19.86.010, *et seq.*)**

296. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

297. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties. Further, the secretly installed Carrier IQ Software embedded on plaintiffs' mobile devices taxes the resources of those mobile devices, including by causing slower performance and decreased battery life. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and their misrepresentations and omissions regarding the privacy and functionality of plaintiffs' mobile devices also constitute unfair or deceptive practices.

298. Defendants' conduct was unfair because it offends established public policy, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair and deceptive trade practices occurred or were committed within defendants' trade or business. Defendants are each directly liable for these violations of law.

299. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

300. Defendants' actions impact the public interest because plaintiffs were injured in exactly the same way as millions of others purchasing and/or using mobile devices as a result of defendants' generalized course of unfair conduct and deception. All of the wrongful conduct alleged herein occurred, continues to occur, and is likely to recur, in the conduct of defendants' business.

301. Plaintiffs and the class were injured as a result of defendant's conduct. Plaintiffs overpaid for their mobile devices and did not receive the benefit of their bargain, and their mobile devices have suffered a diminution in value. Plaintiffs' injury is substantial, is not outweighed by

any countervailing factors, and could not have been reasonably avoided by plaintiffs, as they were not aware of the Carrier IQ Software until well after they had purchased their mobile devices.

302. Defendants' conduct proximately caused the injuries to plaintiffs and the class.

303. Defendants are liable to plaintiffs and the class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

304. Pursuant to Wash. Rev. Code. Ann. § 19.86.095, plaintiffs will serve the Washington Attorney General with a copy of this complaint as plaintiffs seek injunctive relief.

**WEST VIRGINIA  
VIOLATIONS OF THE CONSUMER CREDIT AND PROTECTION ACT  
(W. Va. Code § 46A-1-101, *et seq.*)**

305. Plaintiffs repeat and reallege every allegation above as if set forth herein in full.

306. Defendants are “persons” under W.Va. Code § 46A-1-102(31).

307. Plaintiffs are “consumers,” as defined by W.Va. Code §§ 46A-1- 102(12) and 46A-6-102(2), who purchased or used one or more mobile devices.

308. Defendants participated in unfair or deceptive acts or practices that violated the Consumer Credit and Protection Act (“CCPA”), W. Va. Code § 46A-1- 101, *et seq.*, as described above and below. The CCPA prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce.” W. Va. Code § 46A-6- 104.

309. The conduct of defendants as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, defendants' design and installation of the Carrier IQ Software on mobile devices as described above, which causes the mobile devices to intercept and transmit private information and data to third parties, and causes the mobile devices to suffer reduced battery life and slower performance. Defendants then caused those mobile devices to be sold to consumers, including plaintiffs. Defendants failed to adequately investigate, disclose and remedy the serious security flaws inherent in the Carrier IQ Software, and their misrepresentations and omissions regarding the privacy and functionality of their mobile devices also constitute unfair or deceptive practices.

310. Defendants' conduct was unfair because it offends established public policy, is immoral, unethical, oppressive, and unscrupulous and caused substantial injury to consumers.

including by violation of the state and federal privacy laws enumerated herein. Defendants' unfair and deceptive trade practices occurred or were committed within defendants' trade or business. Defendants are each directly liable for these violations of law.

311. Defendants knew that the mobile devices containing Carrier IQ Software were defectively designed, installed, or manufactured, subjected plaintiffs and other consumers to serious invasions of their privacy, and were not suitable for their intended use. Defendants nevertheless failed to warn plaintiffs about these inherent dangers despite having a duty to do so.

312. Defendants each owed plaintiffs a duty to disclose the defective nature of their mobile devices, including the serious privacy issues presented by the presence of the Carrier IQ Software on the mobile devices, because they: (a) possessed exclusive knowledge of the defects rendering mobile devices inherently more prone to interception and transmission of private information and data than similar mobile devices; (b) intentionally concealed the fact that the mobile devices contained the Carrier IQ Software through their deceptive marketing campaign; and/or (c) made incomplete representations about the privacy and functionality of mobile devices generally, and the Carrier IQ Software in particular, while purposefully withholding material facts from plaintiffs that contradicted these representations.

313. Mobile devices equipped with the Carrier IQ Software cause and pose an unreasonable risk of causing interception and transmission of private information and data, including information and data sent by and/or to third parties.

314. Whether or not a mobile device (a) intercepts private information and data and (b) transmits private information and data to third parties are facts that a reasonable consumer would consider important in selecting a mobile device to purchase or use. When plaintiffs bought a mobile device for personal, family, or household purposes, they reasonably expected the mobile device would (a) not intercept private information and data; and (b) not transmit private information and data to third parties.

315. Defendants' unfair or deceptive acts or practices were likely to deceive reasonable consumers, including plaintiffs, about the true privacy and functionality of their mobile devices.

1           316. As a result of their violations of the CCPA detailed above, defendants caused  
 2 ascertainable loss to plaintiffs and, if not stopped, will continue to harm plaintiffs. Plaintiffs  
 3 currently own or use, or within the class period have owned or used, mobile devices that are  
 4 defective and inherently lacking in privacy protections. The Carrier IQ Software and the resulting  
 5 interceptions, transmissions, and other privacy violations have caused the value of the affected  
 6 mobile devices to plummet.

7           317. Plaintiffs risk irreparable injury as a result of defendants' acts and omissions in  
 8 violation of the CCPA, and these violations present a continuing risk to plaintiffs as well as to the  
 9 general public.

10          318. Defendants' actions impact the public interest because plaintiffs were injured in  
 11 exactly the same way as millions of others purchasing and/or using mobile devices as a result of  
 12 defendants' generalized course of unfair conduct and deception. All of the wrongful conduct  
 13 alleged herein occurred, continues to occur, and is likely to recur, in the conduct of defendants'  
 14 business.

15          319. Pursuant to W. Va. Code § 46A-1-106, plaintiffs seek monetary relief against  
 16 defendants measured as the greater of (a) actual damages in an amount to be determined at trial and  
 17 (b) statutory damages in the amount of \$200 per violation of the CCPA for each plaintiff and each  
 18 member of the class they seek to represent.

19          320. Plaintiffs further seek an order enjoining defendants' unfair or deceptive acts or  
 20 practices, restitution, punitive damages, costs of court, attorneys' fees under W. Va. Code § 46A-5-  
 21 101, *et seq.*, and any other just and proper relief available under the CCPA.

22  
 23  
 24  
 25  
 26  
 27  
 28

**COUNT IV**  
**VIOLATION OF THE MAGNUSON-MOSS WARRANTY ACT**

## (Against the Device Manufacturers)

(On Behalf of Residents of the States of Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming)

321. Plaintiffs repeat and reallege every allegation above as if set forth here in full, including but not limited to the allegations as to breaches of state implied warranties of merchantability as set forth in Count V below.

322. Plaintiffs bring this claim on behalf of themselves and other owners of affected devices who reside in the states of Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.

323. The federal Magnuson-Moss Warranty Act (“MMWA” or “Act”), 15 U.S.C. §§ 2301-2312, is a consumer protection regime designed to supplement state warranty law.

324. The MMWA provides a cause of action for breach of warranty, including the implied warranty of merchantability, or other violations of the Act. 15 U.S.C. § 2310(d)(1). The defendant Device Manufacturers have breached their implied warranties of merchantability - which they cannot disclaim or modify because they offered written warranties to plaintiffs with their devices, 15 U.S.C. § 2308(a)(1) - by failing to provide merchantable goods. The mobile devices at issue are not merchantable or fit for their ordinary purposes because these devices are designed and marketed for communication purposes, including for the transmittal and receipt of confidential, private, and sensitive communication, and yet plaintiffs' and proposed class members' devices do not function accordingly.

325. Rather, these mobile devices, because they bear the Carrier IQ Software, intercept confidential communications and data, including URLs containing HTTP and HTTPS query strings

1 embedded with information such as search terms, user names, passwords, and geo-location  
 2 information; geo-location information apart from that transmitted in URLs; text messages;  
 3 telephone numbers dialed and received; other keystrokes; and application purchases and uses. Most  
 4 of this data is then purposefully captured and transmitted off-device as a function of the Carrier IQ  
 5 Software.

6       326. Furthermore, with respect to HTC devices, and on information and belief, possibly  
 7 with respect to certain other devices, all such material is being captured in unencrypted, human-  
 8 readable form in device debug logs, or logs, such that it is being transmitted to Google and likely to  
 9 third-party application developers and vendors along with crash reports, and such that it is  
 10 vulnerable to other third-parties with potentially malicious intent or to anyone with access to the  
 11 logs. With respect to the allegations contained in this paragraph, plaintiffs bring them only against  
 12 HTC at this time.

13       327. Additionally, the Carrier IQ Software that the Device Manufacturers secretly  
 14 installed on the mobile devices at issue depletes battery power and life. Battery power is the  
 15 lifeblood of mobile devices; without it, devices cannot fulfill their ordinary purposes. Here, battery  
 16 power is used for the processing and transmitting that the Carrier IQ Software performs on the  
 17 mobile devices. Indeed, it is plausible that the precise level of discharge can be discerned via the  
 18 Carrier IQ Software itself, given its reporting capabilities. Furthermore, operation of the Carrier IQ  
 19 Software placed on the devices reduced the utility and lifespan of device batteries because each  
 20 charge and use cycle diminishes a battery's storage capacity, a consequence of which is the need  
 21 for more frequent discharges.

22       328. Plaintiffs and proposed class members have suffered damages as a result of the  
 23 Device Manufacturers', or where qualified, HTC's, breaches of their implied warranties as set forth  
 24 herein. Accordingly, this action lies under the MMWA. 15 U.S.C. § 2310(d)(1)-(2).

25       329. In addition, the Device Manufacturers', or where qualified, HTC's, acts and  
 26 omissions in violation of the Act are “[u]nfair methods of competition in or affecting commerce,  
 27 and unfair or deceptive acts or practices in or affecting commerce,” and they are unlawful. 15  
 28 U.S.C. § 2310(b); 15 U.S.C. § 45(a)(1).

330. The MMWA provides for “damages and other legal and equitable” relief where there has been a breach of warranty or failure to abide by the obligations that the Act imposes. 15 U.S.C. § 2310(d)(1). As set forth more fully in Count VII below, plaintiffs and prospective class members seek damages in the amount of full refunds for their mobile devices, based on the differential between the value of the goods as tendered to them and the value they would have had if they had been as impliedly warranted.

331. In addition, or in the alternative, plaintiffs and the class they seek to represent ask for equitable relief in the form of an order against all Device Manufacturers requiring them to conform the mobile devices here at issue to the implied warranties made with respect to them by requiring cessation of the interception, reading, capturing, logging, and transmittals of personal, private, confidential, and sensitive communications and data as alleged in this complaint.

332. The MMWA also provides for an award of costs and expenses, including attorneys' fees, to prevailing consumers in connection with the commencement and prosecution of lawsuits thereunder, unless the Court in its discretion determines that such an award would be inappropriate. 15 U.S.C. § 2310(d)(2). Plaintiffs and prospective class members intend to seek such an award, including expert witness costs and other recoverable costs, as prevailing consumers at the conclusion of this lawsuit.

**COUNT V**  
**VIOLATION OF THE IMPLIED WARRANTY OF MERCHANTABILITY**

(Against the Device Manufacturers)

(On Behalf of Residents of the States of Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming)

333. Plaintiffs repeat and reallege every allegation above as if set forth here in full.

334. Plaintiffs bring this claim for breach of the Uniform Commercial Code's implied warranty of merchantability on behalf of themselves and other owners of affected devices who reside in the states of Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi,

1 Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota,  
 2 Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia,  
 3 Washington, West Virginia, and Wyoming.

4       335. The defendant Device Manufacturers are merchants as defined by applicable UCC  
 5 provisions.

6       336. Though privity is not required under the law of the referenced states, plaintiffs and  
 7 the class were in privity with the Device Manufacturers in that they purchased their mobile devices  
 8 from actual or apparent agents of the Device Manufacturers, such as the Device Manufacturers'  
 9 authorized dealers.

10      337. Further, though privity is not required under the law of the referenced states,  
 11 plaintiffs and the class were and are also in privity with the Device Manufacturers by virtue of the  
 12 contractual relationship stemming from the Device Manufacturers' written warranties provided in  
 13 conjunction with the purchase of their mobile devices, which are enforceable by plaintiffs and the  
 14 class as against the Device Manufacturers, regardless of where, or from whom, the Device  
 15 Manufacturers' products were acquired. Further, or in the alternative, plaintiffs and the class  
 16 members were intended third-party beneficiaries of the Device Manufacturers' contract for sale of  
 17 devices to the persons or entities from whom plaintiffs and the class ultimately purchased their  
 18 mobile devices.

19      338. The Device Manufacturers have breached the implied warranties of merchantability  
 20 that they made to plaintiffs and the prospective class. To illustrate the Device Manufacturers'  
 21 breaches, using California law as an example: the Device Manufacturers impliedly warranted to  
 22 plaintiffs and prospective class members that their mobile devices were free of defects, that they  
 23 were merchantable, and that they were fit for the ordinary purpose for which such goods are used.  
 24 *See, e.g., Cal. Com. Code § 2314* (setting forth, as codified in California, the UCC's implied  
 25 warranty of merchantability). The ordinary purpose of mobile devices such as those at issue is  
 26 communication, including confidential and private communications via the Internet and with  
 27 others, via telephone calls and text messages. In addition, an ordinary use of devices such as these  
 28 is the purchase and use of applications. The Device Manufacturers impliedly represented to

1 plaintiffs and prospective class members that the mobile devices at issue were free of defects that  
 2 could impinge on these ordinary uses, that they were merchantable with respect to such uses, and  
 3 that they were fit for all such purposes.

4       339. As alleged herein, however, the Device Manufacturers' sales of mobile devices  
 5 breached the implied warranty of merchantability because the devices were defective,  
 6 unmerchantable, and not fit for the ordinary purpose for which such goods are used. More  
 7 specifically, all mobile devices bearing the Carrier IQ Software are defective and unfit for their  
 8 ordinary purposes because, rather than performing as impliedly represented, these devices instead  
 9 intercept URLs containing HTTP and HTTPS query strings embedded with information such as  
 10 search terms, user names, passwords, and geo-location information; geo-location information apart  
 11 from that transmitted in URLs; text messages; telephone numbers dialed and received; other  
 12 keystrokes; and application purchases and uses. These devices then store most of this information  
 13 in device memory, unbeknownst to consumers, before transmitting such information, save for SMS  
 14 text message content and certain other keystrokes, to Carrier IQ and/or wireless carriers and/or  
 15 device manufacturers.

16       340. HTC's - and, on information and belief, possibly other device manufacturers' - sales  
 17 of mobile devices additionally breached the implied warranty of merchantability because for other  
 18 important reasons, the devices were defective, unmerchantable, and not fit for the ordinary purpose  
 19 for which these goods are used. More specifically, HTC mobile devices bearing Carrier IQ  
 20 Software are defective, unmerchantable, and unfit for their ordinary purposes because they  
 21 intercept URLs containing HTTP and HTTPS query strings embedded with information such as  
 22 search terms, user names, passwords, and geo-location information; geo-location information apart  
 23 from that transmitted in URLs; text messages; telephone numbers dialed and received; other  
 24 keystrokes; and application purchases and uses, and then they store this content and information in  
 25 unencrypted, human-readable form in the mobile devices' debug logs, unbeknownst to consumers,  
 26 before transmitting all such information, including SMS text message content, to Google and  
 27 possibly third-party application developers and vendors, when the devices or applications crash.  
 28 Moreover, this unencrypted, human-readable content is vulnerable to other third-parties with

1 potentially malicious intent or to anyone with access to the logs. Investigation continues as which  
 2 other mobile devices are so affected.

3       341. Additionally, the Device Manufacturers breached their implied warranties of  
 4 merchantability because the Carrier IQ Software secretly installed on plaintiffs' and prospective  
 5 class members' mobile devices depletes battery power and life. Battery power is the lifeblood of  
 6 mobile devices; without it, devices cannot fulfill their ordinary purposes. Here, battery power is  
 7 used for the processing and transmitting that Carrier IQ Software performs on the mobile devices.  
 8 Indeed, it is plausible that the precise level of discharge can be discerned via Carrier IQ Software  
 9 itself, given its reporting capabilities. Furthermore, operation of the Carrier IQ Software placed on  
 10 the devices reduced the utility and lifespan of device batteries because each charge and use cycle  
 11 diminishes a battery's storage capacity, a consequence of which is the need for more frequent  
 12 discharges.

13       342. The Device Manufacturers have had reasonable and adequate notice of plaintiffs'  
 14 and the class's – i.e., consumers', rather than commercial parties' - claims for breach of implied  
 15 warranty of merchantability, including by way of the individual suits that preceded filing of either  
 16 consolidated amended complaint, by way of numerous reports of these breaches likely made to  
 17 them directly, by way of Mr. Eckhart's and other publications which preceded the filing of  
 18 plaintiffs' suits, and by way of the numerous press reports published before plaintiffs filed suit  
 19 against them. Yet then and to-date, the Device Manufacturers have demonstrated no willingness to  
 20 negotiate toward making the plaintiffs and the class whole. Furthermore, to the extent notice might  
 21 be required under any reading of applicable law, any such notice would not be required to go to the  
 22 Device Manufacturers, but rather, only to the direct sellers of plaintiffs' and the class's mobile  
 23 devices, and the direct sellers are not defendants in this action.

24       343. Any purported modifications or limitations of the implied warranty of  
 25 merchantability, including by way of terms set forth in the Device Manufacturers' written  
 26 warranties, are invalid, void, and unenforceable per the MMWA. 15 U.S.C. § 2308(a)(1).

27       344. As a result of the Device Manufacturers' breaches of their implied warranties of  
 28 merchantability, plaintiffs and other owners of affected devices who reside in the states of Alaska,

1 Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas,  
 2 Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri,  
 3 Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota,  
 4 Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia,  
 5 Washington, West Virginia, and Wyoming have been injured and are entitled to the full panoply of  
 6 remedies provided under Article 2 of the UCC as adopted by the various states, as well as all other  
 7 applicable remedies. These include, including under California law specifically, monetary  
 8 damages. *See, e.g.*, Cal. Com. Code § 2714. Because of the defects in the mobile devices and their  
 9 behavior as described herein, there was no value to the goods as accepted. The value of these  
 10 devices had they been as warranted may be measured by their purchase prices; accordingly,  
 11 damages in the sums of their purchase prices, or as otherwise measured pursuant to the damages  
 12 provisions of Article 2 of the UCC, are warranted to plaintiffs and members of the proposed class.  
 13 *See, e.g.*, Cal. Com. Code § 2714(2).

14       345. With regard to the states other than California, plaintiffs allege as follows:

15       346. Plaintiffs again incorporate by reference all allegations of the preceding paragraphs  
 16 as though fully set forth herein.

17       347. Defendants are and were at all relevant times merchants with respect to mobile  
 18 devices under Alaska Stat. § 45.02.104, Ark. Code § 4-1-2, Ala. Code § 7-2-104, Colo. Rev. Stat. §  
 19 4-2-104, 6 Del. Code § 2-104, D.C. Code § 28:2-104, Haw. Rev. Stat. § 490:2-104, Ind. Code Ann.  
 20 § 26-1-2-104, Kan. Stat. § 84-2-104, Me. Rev. Stat. § 11. 2-104, Md. Com. Law Code § 2-104,  
 21 Mass. Gen. laws Ch. 106, § 2-104, Mich. Stat. § 440.2104, Minn. Stat. § 336.2-104, Miss. Code  
 22 Ann. § 75-2-104, Vernon's Mo. Rev. Stat. § 400.2-104, Mont. Code Ann. § 30-2-104, Neb. Rev.  
 23 Stat. § UCC-2-104, Nev. Rev. Stat. § 104.2104, N.H. Rev. Stat. § 382-A:2-104, N.J. Stat. Ann. §  
 24 12A:2-104, N.M. Stat. Ann. § 55-2-104, N.D. Cent. Code § 41-02-01, Okla. Stat. tit. § 12A-2-104,  
 25 13 Pa. Stat. Ann. § 2104, R.I. Gen. Laws. § 6A-2-104, S.C. Code Laws § 36-2-104, S.D. Code  
 26 Laws § 57A-2-104, Tex. Bus. & Com. Code § 2.104, Utah Code Ann. § 70A-2-104, VA. Code  
 27 Ann. § 8.2-104, Wash. Rev. Code § 62A.2-104, W. Va. Code § 46-2-104, Wyo. Stat. § 34.1-2-104.

1           348. A warranty that the mobile devices were in merchantable condition was implied by  
 2 law in the instant transaction, pursuant to Alaska Stat. § 45.02.314, Ark. Code § 4-1-2, Ala. Code §  
 3 7-2-314, Colo. Rev. Stat. § 4-2-314, 6 Del. Code § 2-314, D.C. Code § 28:2-314, Haw. Rev. Stat. §  
 4 490:2-314, Ind. Code Ann. § 26-1-2-314, Kan. Stat. § 84-2-314, Me. Rev. Stat. § 11. 2-314, Md.  
 5 Com. Law Code § 2-314, Mass. Gen. laws Ch. 106, § 2-314, Mich. Stat. § 440.2314, Minn. Stat. §  
 6 336.2-314, Miss. Code Ann. § 75-2-314, Vernon's Mo. Rev. Stat. § 400.2-314, Mont. Code Ann. §  
 7 30-2-314, Neb. Rev. Stat. § UCC-2-314, Nev. Rev. Stat. § 104.2314, N.H. Rev. Stat. § 382-A:2-  
 8 314, N.J. Stat. Ann. § 12A:2-314, N.M. Stat. Ann. § 55-2-314, N.D. Cent. Code § 41-02-01, Okla.  
 9 Stat. tit. § 12A-2-314, 13 Pa. Stat. Ann. § 2314, R.I. Gen. Laws. § 6A-2-314, S.C. Code Laws § 36-  
 10 2-314, S.D. Code Laws § 57A-2-314, Tex. Bus. & Com. Code § 2.314, Utah Code Ann. § 70A-2-  
 11 314, Va. Code Ann. § 8.2-314, Wash. Rev. Code § 62A.2-314, W. Va. Code § 46-2-314, Wyo.  
 12 Stat. § 34.1-2-314.

13           349. These mobile devices, when sold and at all times thereafter, were not in  
 14 merchantable condition and are not fit for the ordinary purpose for which mobile devices are used.  
 15 Specifically, the mobile devices are inherently defective in that defendants installed the Carrier IQ  
 16 Software on those mobile devices, which causes the mobile devices to intercept and transmit  
 17 certain private information and data from the mobile devices. The mobile devices with the Carrier  
 18 IQ Software were not adequately designed, manufactured, and tested.

19           350. Defendants were provided notice of these issues by numerous complaints filed  
 20 against it, including this Complaint, and by numerous individual letters, telephone calls, and other  
 21 communications sent by plaintiffs and other class members before or within a reasonable amount  
 22 of time after the Carrier IQ-related defects became public, as well as letters from Senator Franken.

23           351. Plaintiffs and the other class members have had sufficient direct dealings with either  
 24 defendants or their agents to establish privity of contract between plaintiffs and the other class  
 25 members. Notwithstanding this, privity is not required in this case because plaintiffs and the other  
 26 class members are intended third-party beneficiaries of contracts between defendants and their  
 27 distributors, and between defendants and certain wireless carriers; specifically, they are the  
 28 intended beneficiaries of defendants' implied warranties. The distributors and carriers were not

1 intended to be the ultimate consumers of the mobile devices and have no rights under the warranty  
 2 agreements provided with the mobile devices; the warranty agreements were designed for and  
 3 intended to benefit the ultimate consumers only.

4       352. As a direct and proximate result of defendants' breaches of the warranties of  
 5 merchantability, plaintiffs and the other class members have been damaged in an amount to be  
 6 proven at trial.

7           **Breach of implied warranty under the Song-Beverly Consumer Warranty Act**

8       353. Additionally, plaintiffs and the other class members who purchased mobile devices  
 9 in California are "buyers" within the meaning of Cal. Civ. Code § 1791(b) of the Song-Beverly  
 10 Consumer Warranty Act.

11       354. The mobile devices are "consumer goods" within the meaning of Cal. Civ. Code §  
 12 1791(a).

13       355. Defendants are "manufacturers" of the mobile devices within the meaning of Cal.  
 14 Civ. Code § 1791(j).

15       356. Defendants impliedly warranted to plaintiffs and the other class members that their  
 16 mobile devices were "merchantable" within the meaning of Cal. Civ. Code §§ 1791.1(a) & 1792,  
 17 however, the mobile devices do not have the quality that a buyer would reasonably expect.

18       357. Cal. Civ. Code § 1791.1(a) states:

19           "Implied warranty of merchantability" or "implied warranty that goods are merchantable"  
 20 means that the consumer goods meet each of the following:

- 21       (1) Pass without objection in the trade under the contract description.
- 22       (2) Are fit for the ordinary purposes for which such goods are used.
- 23       (3) Are adequately contained, packaged, and labeled.
- 24       (4) Conform to the promises or affirmations of fact made on the container or label.

25       358. The mobile devices would not pass without objection in the mobile device trade  
 26 because of the defects in the mobile devices, specifically relating to the installation and operation  
 27 of the Carrier IQ Software, which cause the mobile devices to intercept and transmit private  
 28 information and data from the mobile devices.

1           359. Because of the defects in the mobile devices which cause the mobile devices to  
 2 intercept and transmit private information and data from the mobile devices, they are not secure to  
 3 use and thus not fit for ordinary purposes.

4           360. The mobile devices are not adequately labeled because the labeling fails to disclose  
 5 the defects in the mobile devices which cause the mobile devices to intercept and transmit private  
 6 information and data from the mobile devices.

7           361. Defendants breached the implied warranty of merchantability by manufacturing and  
 8 selling mobile devices containing defects associated with the Carrier IQ Software, consisting of the  
 9 Carrier IQ Software. Furthermore, these defects have caused plaintiffs and the other class members  
 10 to not receive the benefit of their bargain and have caused mobile devices to depreciate in value.

11          362. As a direct and proximate result of defendants' breach of the implied warranty of  
 12 merchantability, plaintiffs and the other class members received goods whose defective and  
 13 dysfunctional condition substantially impairs their value to plaintiffs and the other class members.  
 14 Plaintiffs and the other class members have been damaged as a result of the diminished value of  
 15 defendants' products, the products' malfunctioning, and the nonuse of their mobile devices.

16          363. Pursuant to Cal. Civ. Code §§ 1791.1(d) & 1794, plaintiffs and the other class  
 17 members are entitled to damages and other legal and equitable relief including, at their election, the  
 18 purchase price of their mobile devices, or the overpayment or diminution in value of their mobile  
 19 devices.

20           **Louisiana**

21          364. As for the claims of Louisiana residents, the Civil Code of that state provides  
 22 implied warranty protections, and, as a direct and proximate result of defendants' breaches of those  
 23 protections, plaintiffs and the other class members have been damaged in an amount to be proven  
 24 at trial.

25           **VII. PRAYER FOR RELIEF**

26          WHEREFORE, plaintiffs respectfully request the following relief:

27          A. That the Court certify the requested class, and that it appoint the named plaintiffs to  
 28 be class representatives and interim co-lead counsel to be class counsel;

1           B.       That the Court award plaintiffs and the class(es) appropriate relief, to include  
2 damages, including statutory damages, as requested herein;

3           C.       That the Court award plaintiffs and the class(es) injunctive or other equitable or  
4 declaratory relief as requested herein and as may be appropriate otherwise under applicable state or  
5 federal law;

6           D.       That the Court issue such additional orders or judgments as may be necessary to  
7 prevent the practices of which plaintiffs complain and to restore to any person in interest any  
8 money or property which may have been acquired by means of state consumer protection act  
9 violations;

10          E.       That the Court award plaintiffs and the class(es) their costs, including expert witness  
11 costs pursuant to the MMWA and as otherwise available, as well as reasonable attorneys' fees as  
12 available under the laws cited above;

13          F.       That the Court award plaintiffs and the class(es) such other, favorable relief as may  
14 be available and appropriate under federal or state law, or at equity.

15

16

17

18

19

20

21

22

23

24

25

26

27

28

## **VIII. JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury on all issues so triable.

DATED: June 23, 2014.

## HAGENS BERMAN SOBOL SHAPIRO LLP

By /s/ Robert F. Lopez

Steve W. Berman (*pro hac vice*)  
Robert F. Lopez (*pro hac vice*)  
HAGENS BERMAN SOBOL SHAPIRO LLP  
1918 Eighth Avenue, Suite 3300  
Seattle, WA 98101  
Telephone: (206) 623-7292  
Facsimile: (206) 623-0594  
[steve@hbsslaw.com](mailto:steve@hbsslaw.com)  
[robl@hbsslaw.com](mailto:robl@hbsslaw.com)

PEARSON SIMON & WARSHAW, LLP

By        /s/ Bruce L. Simon

Bruce L. Simon (96241)  
William J. Newsom (267643)  
44 Montgomery Street, Suite 2450  
San Francisco, CA 94104  
Telephone: (415) 433-9000  
Facsimile: (415) 433-9008  
[bsimon@pswlaw.com](mailto:bsimon@pswlaw.com)  
[wnewsom@pswlaw.com](mailto:wnewsom@pswlaw.com)

Clifford H. Pearson (108523)  
Daniel L. Warshaw (185365)  
15165 Ventura Blvd., Suite 400  
Sherman Oaks, CA 91403  
Telephone: (818) 788-8300  
[cpearson@pswlaw.com](mailto:cpearson@pswlaw.com)  
[dwarshaw@pswlaw.com](mailto:dwarshaw@pswlaw.com)

*Counsel for Select Plaintiffs and  
Co-Lead Counsel for the Proposed Classes*

1 J. Paul Gignac  
2 Helen Kim  
3 ARIAS OZZELLO & GIGNAC LLP  
4 115 S. La Cumbre Lane, Suite 300  
5 Santa Barbara, California 93105  
6 Telephone: (805) 683-7400  
7 Facsimile: (805) 683-7401  
8 hkim@aogllp.com  
9 j.paul@aogllp.com

10 Rosemary M. Rivas  
11 Danielle A. Stoumbos  
12 FINKELSTEIN THOMPSON LLP  
13 505 Montgomery Street, Suite 300  
14 San Francisco, California 94111  
15 Telephone: (415) 398-8700  
16 Facsimile: (415) 398-8704  
dstoumbos@finkelsteinthompson.com  
rrivas@finkelsteinthompson.com

17 Eric D. Holland  
18 HOLLAND GROVES SCHNELLER STOLZE LLC  
19 300 N. Tucker Blvd., Suite 801  
20 Saint Louis, MO 63101  
21 Telephone: 314-241-8111  
Facsimile: 314-241-5554  
eholland@gsslaw.com

22 Paul R. Kiesel  
23 KIESEL LAW LLP  
24 8648 Wilshire Boulevard  
25 Beverly Hills, CA 90211  
26 Telephone: (310) 854-4444  
Facsimile: (310) 854-0812  
kiesel@kbla.com

27 Charles E. Schaffer  
28 LEVIN, FISHBEIN, SEDRAN &  
BERMAN  
510 Walnut Street, Suite 500  
Philadelphia, PA 19106  
Telephone: (215) 592-1500  
Facsimile: (215) 592-4663  
cschaffer@lfsblaw.com

*Executive Committee Members for the Proposed Class*

**CERTIFICATE OF SERVICE**

I hereby certify that on June 23, 2014, I electronically filed the foregoing document using the CM/ECF system which will send notification of such filing to the e-mail addresses registered in the CM/ECF system, as denoted on the Electronic Mail Notice List, and I hereby certify that I have caused to be mailed a paper copy of the foregoing document via the United States Postal Service to the non-CM/ECF participants indicated on the Manual Notice List generated by the CM/ECF system.

Dated: June 23, 2014

/s/ William J. Newsom

---

William J. Newsom  
44 Montgomery Street, Suite 2450  
San Francisco, CA 94104  
Telephone: (415) 433-9000  
Facsimile: (415) 433-9008  
wnewsom@pswlaw.com

**ATTESTATION PURSUANT TO LOCAL RULE 5-1(i)(3)**

I, William J. Newsom, am the ECF User whose identification and password are being used to file this **SECOND CONSOLIDATED AMENDED COMPLAINT**. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that all signatories have concurred in this filing.